McAfee®

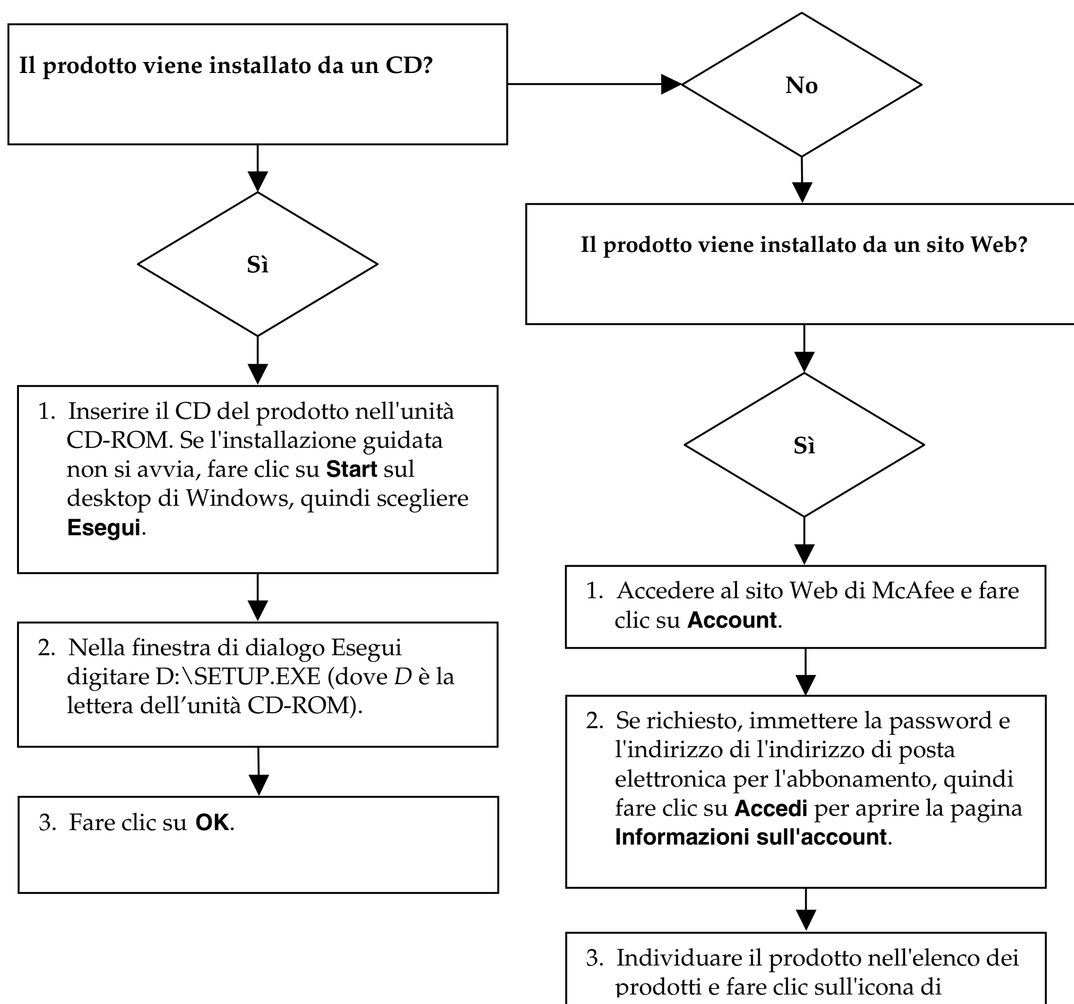
wirelesshomenetworksecurity suite

Guida dell'utente

McAfee®

Scheda di avvio rapido

Se si installa il prodotto dal CD o dal sito Web, stampare questa pratica pagina di riferimento.



Per ulteriori informazioni

Per visualizzare le Guide dell'utente sul CD del prodotto, controllare che Acrobat Reader sia installato; in caso contrario, installarlo dal CD del prodotto McAfee.

1. Inserire il CD del prodotto nell'unità CD-ROM.
2. Aprire Esplora risorse: Fare clic su **Start** sul desktop di Windows, quindi su **Cerca**.
3. Individuare la cartella Manuali e fare doppio clic sul file .PDF della Guida dell'utente che si desidera aprire.

Vantaggi della registrazione

Per inviare la registrazione direttamente a McAfee, si consiglia di attenersi alla facile procedura contenuta nel prodotto acquistato. Oltre a garantire supporto tecnico puntuale e competente, la registrazione offre i seguenti vantaggi:

- Supporto elettronico GRATUITO
- Aggiornamenti dei file di definizione dei virus (.DAT) per un anno dall'installazione quando si acquista il software VirusScan

  Per informazioni sui prezzi di un ulteriore anno di abbonamento per gli aggiornamenti delle definizioni dei virus, visitare il sito http://it.mcafee.com

- 60 giorni di garanzia per l'eventuale sostituzione del CD del software nel caso in cui sia difettoso o danneggiato
- Aggiornamenti dei filtri di SpamKiller per un anno dall'installazione quando si acquista il software SpamKiller

  Per informazioni sui prezzi di un ulteriore anno di abbonamento per gli aggiornamenti dei filtri, visitare il sito http://it.mcafee.com

- Aggiornamenti di McAfee Internet Security Suite per un anno dall'installazione quando si acquista il software MIS

  Per informazioni sui prezzi di un ulteriore anno di abbonamento per gli aggiornamenti dei contenuti, visitare il sito http://it.mcafee.com

Supporto tecnico

Per il supporto tecnico, visitare il sito http://www.mcafeeaiuto.com/.

Il sito del supporto tecnico consente di accedere 24 ore su 24 alla semplice procedura di risposta guidata alle domande più comuni.

Gli utenti più esperti possono anche provare le opzioni avanzate, tra cui una ricerca basata su parole chiave e un sistema di Guida in linea. Se non si trova una soluzione, si può inoltre accedere alle opzioni GRATUITE di chat e posta elettronica. Le opzioni di chat e posta elettronica consentono di entrare rapidamente in contatto tramite Internet con i tecnici qualificati del servizio di supporto, senza costi aggiuntivi. In alternativa, le informazioni sull'assistenza telefonica sono reperibili presso il sito http://www.mcafeeaiuto.com/.

Sommario

Guida introduttiva 1

Internet offre una grande quantità di informazioni e attività di intrattenimento a portata di mouse. Tuttavia, appena ci si collega, si espone il computer a un gran numero di minacce per la sicurezza e la riservatezza. Proteggere la rete senza fili, il computer e i dati con McAfee Wireless Home Network Security Suite. Grazie alle tecnologie d'avanguardia di McAfee Wireless Home Network Security, McAfee VirusScan e McAfee Personal Firewall Plus, Wireless Home Network Security Suite costituisce uno dei pacchetti più completi per la protezione della privacy e della sicurezza presenti sul mercato.

Per ulteriori informazioni sui prodotti McAfee, vedere i seguenti capitoli:

- *McAfee Wireless Home Network Security* a pagina 11
- *McAfee VirusScan* a pagina 49
- *McAfee Personal Firewall Plus* a pagina 85

Requisiti di sistema

- Microsoft® Windows 98SE, Windows Me, Windows 2000 o Windows XP
- PC con processore compatibile Pentium

  Windows 98 o 2000: 133 MHz o superiore

  Windows Me: 150 MHz o superiore

  Windows XP (Home e Pro): 300 MHz o superiore
- RAM

  Windows 98SE, Me o 2000: 64 MB

  Windows XP (Home e Pro): 128 MB
- 100 MB di spazio sul disco rigido
- Microsoft Internet Explorer 5.5 o versione successiva

  NOTA
  Per eseguire l'aggiornamento all'ultima versione di Internet Explorer, visitare il sito Web di Microsoft, all'indirizzo http://www.microsoft.com/.

Rete senza fili

- Adattatore di rete senza fili standard
- Router o access point senza fili standard, inclusi gran parte dei modelli Linksys®, NETGEAR®, D-Link® e Belkin®

Programmi di posta elettronica supportati

- POP3 (Outlook Express, Outlook, Eudora, Netscape)

Programmi di messaggistica immediata supportati:

- AOL Instant Messenger 2.1 o versioni successive
- Yahoo Messenger 4.1 o versioni successive
- Microsoft Windows Messenger 3.6 o versioni successive
- MSN Messenger 6.0 o versioni successive

Utilizzo di McAfee SecurityCenter

McAfee SecurityCenter è un punto di riferimento unico per la protezione. L'integrazione trasparente con McAfee SecurityCenter fornisce un quadro completo dello stato di protezione del sistema, nonché i più recenti avvisi sui virus e sulla protezione. È possibile eseguire SecurityCenter dall'icona McAfee nella barra delle applicazioni di Windows oppure dal desktop di Windows.

> **NOTA**
> Per ulteriori informazioni sulle funzioni, fare clic su **?** nella finestra di dialogo di SecurityCenter.

Quando SecurityCenter è in esecuzione e tutte le funzioni di McAfee installate nel sistema sono attivate, nella barra delle applicazioni di Windows viene visualizzata un'icona raffigurante una **M** rossa (area di notifica di Windows XP).

In caso di disattivazione di una o più applicazioni McAfee installate nel sistema, l'icona McAfee risulterà di colore nero: .

Per aprire McAfee SecurityCenter:

1. Fare clic con il pulsante destro del mouse sull'icona McAfee .
2. Fare clic su **Apri SecurityCenter**.

Per accedere al prodotto McAfee desiderato:

1. Fare clic con il pulsante destro del mouse sull'icona McAfee .
2. Scegliere il prodotto McAfee desiderato e selezionare la funzione da utilizzare.

McAfee Wireless Home Network Security 2

Benvenuti in McAfee Wireless Home Network Security, che offre protezione avanzata per la rete senza fili, i dati personali e il computer.

Questo prodotto è progettato per computer con connessioni senza fili. Quando si installa questo prodotto su computer che si connettono a una rete mediante cavo, non si dispone delle funzionalità complete sui computer cablati.

McAfee Wireless Home Network Security migliora la privacy durante l'utilizzo del computer crittografando i dati personali e privati mentre vengono inviati sulla rete senza fili protetta e impedisce agli hacker di accedere alle informazioni.

Utilizzo di McAfee Wireless Home Network Security

Prima di proteggere la rete, considerare quanto segue.

- Connessioni tramite cavo: i computer connessi al router mediante un cavo non necessitano di protezione, dato che i segnali trasmessi su un cavo non possono essere intercettati.
- Connessioni senza fili: i computer che dispongono di connessioni senza fili vanno protetti perché i dati possono essere intercettati. È necessario utilizzare un computer senza fili per proteggere una rete, perché soltanto un computer senza fili può concedere l'accesso a un altro computer senza fili.

Protezione della rete

Non è necessario proteggere la rete se si effettua la connessione tramite cavo.

1. Sul computer senza fili, installare l'adattatore senza fili e verificare che sia abilitato. L'adattatore senza fili può essere una scheda inserita a lato del computer oppure una porta USB. Molti computer di nuova generazione sono dotati di un adattatore senza fili incorporato, pertanto, non è necessario installarlo.
2. Installare il router o l'access point senza fili (gli access point vengono utilizzati per estendere il raggio d'azione della rete senza fili) e verificare che sia acceso e abilitato. Per una definizione più completa di router e access point, vedere il *Glossario* a pagina 38.

3 Installare McAfee Wireless Home Network Security su ciascun computer senza fili nella rete. Non è necessario installare questo software sui computer connessi tramite cavo. Vedere *Installazione di Wireless Home Network Security* a pagina 14.

4 Da uno dei computer senza fili, proteggere la rete. Vedere *Protezione delle reti senza fili* a pagina 24.

5 Aggiungersi alla rete da altri computer senza fili. Vedere *Protezione di altri computer* a pagina 23.

Informazioni su Wireless Home Network Security

Spesso si utilizza la rete senza fili a casa perché è semplice e conveniente. La tecnologia senza fili consente di accedere a Internet da qualsiasi stanza della casa o addirittura dal cortile, senza il costo e il fastidio dei cavi. Le reti senza fili facilitano l'accesso alla rete da parte di parenti e amici.

Tuttavia, questa convenienza comporta una certa vulnerabilità della protezione. Le reti senza fili utilizzano onde radio per trasmettere i dati e queste onde sono in grado di attraversare le pareti casa. Con l'ausilio di antenne specializzate, è possibile che degli intrusi accedano alla rete senza fili o intercettino i dati a chilometri di distanza.

Per proteggere la rete senza fili e i dati, è necessario restringere l'accesso alla rete senza fili e crittografare i dati. Il router o l'access point senza fili è dotato di standard di protezione incorporati ma la difficoltà è rappresentata dall'attivazione e dalla gestione corretta delle impostazioni di protezione. Oltre il 60% delle reti senza fili non utilizza un livello di protezione elevato come la crittografia.

Wireless Home Network Security facilita l'utilizzo

McAfee Wireless Home Network Security attiva la protezione sulla rete senza fili e protegge le informazioni inviate con una semplice procedura che, con un solo clic, consente di generare automaticamente una chiave di crittografia. La maggior parte delle chiavi facili da ricordare possono essere decifrate velocemente dagli hacker. Consentendo al computer di memorizzare la chiave, Wireless Home Network Security può utilizzare chiavi impossibili da decifrare.

Questo software, eseguito continuamente in background, consente inoltre di creare e distribuire una nuova chiave di crittografia ogni pochi minuti, dimostrandosi efficace anche contro gli hacker più determinati. I computer autorizzati, come quelli di parenti e amici che desiderano avere accesso alla rete senza fili, ricevono una chiave di crittografia e tutte le distribuzioni delle chiavi.

Questa procedura garantisce una protezione efficace e al contempo può essere implementata facilmente a casa dal proprietario di una rete senza fili. Con un solo clic, è possibile impedire agli hacker di rubare i dati trasmessi senza fili. Gli hacker non potranno inserire cavalli di Troia o altro malware sulla rete. È inoltre non potranno utilizzare la rete senza fili come piattaforma per il lancio di attacchi di spam o di virus. Anche eventuali freeloader occasionali che potrebbero utilizzare la rete per il download illegale di film e canzoni verranno bloccati, evitando il fastidio di errati carichi di responsabilità per azioni illegali.

Altre soluzioni non offrono la semplicità o l'efficacia della protezione offerta da Wireless Home Network Security. L'applicazione di filtri agli indirizzi MAC o la disattivazione della trasmissione SSID offre solo una protezione superficiale. Anche gli hacker più inesperti sono in grado di forzare questi meccanismi, utilizzando strumenti scaricabili gratuitamente da Internet. Altre utilità, quali le reti VPN non proteggono la rete senza fili, lasciando gli utenti vulnerabili a numerosi attacchi.

McAfee Wireless Home Network Security è il primo prodotto che rende inattaccabili le reti domestiche senza fili.

Funzioni

Questa versione di Wireless Home Network Security offre le seguenti funzioni:

- Protezione sempre attiva: rileva e protegge automaticamente qualsiasi rete senza fili vulnerabile a cui ci si è connessi.
- Interfaccia intuitiva: è possibile proteggere la rete senza dover prendere decisioni difficili o conoscere termini tecnici complessi.
- Crittografia automatica potente: consente l'accesso alla rete solo a parenti e amici e protegge la trasmissione e la ricezione dei dati.
- Soluzione solo software: Wireless Home Network Security funziona con router o access point senza fili standard e il software per la protezione. Non è necessario acquistare hardware addizionale.
- Rotazione automatica della chiave: persino gli hacker più determinati non possono acquisire le informazioni, poiché la chiave è in continua rotazione.
- Aggiunta di utenti di rete: è possibile autorizzare parenti e amici ad accedere alla rete.
- Strumento di connessione intuitivo: strumento di connessione senza fili intuitivo e informativo, con dettagli sulla potenza del segnale e sullo stato della protezione.
- Registrazione di eventi e avvisi: segnalazioni e avvisi di facile comprensione offrono agli utenti più esperti ulteriori informazioni sulla rete senza fili.

- Modalità sospensione: è possibile sospendere temporaneamente la rotazione della chiave in modo che particolari applicazioni possano funzionare senza interruzione.
- Compatibilità con altri dispositivi: Wireless Home Network Security si aggiorna automaticamente con i moduli di router o access point senza fili più recenti delle marche più diffuse, inclusi: Linksys®, NETGEAR®, D-Link®, Belkin® e altri.

Installazione di Wireless Home Network Security

Questa sezione spiega come installare Wireless Home Network Security e fornisce una guida introduttiva su come proteggere la rete.

Quando si installa McAfee Wireless Home Network Security, considerare quanto segue.

- Installare questo software su tutti i computer senza fili.
- Non è necessario installare questo software sui computer connessi tramite cavo.

Installazione dal CD

1. Inserire il CD del prodotto nell'unità CD-ROM. Se l'installazione non viene avviata automaticamente, fare clic su **Start** sul desktop di Windows, quindi su **Esegui**.
2. Nella finestra di dialogo **Esegui**, digitare D:\SETUP.EXE (dove D è la lettera corrispondente all'unità CD-ROM).
3. Fare clic su **OK**.
4. Andare a *Utilizzo della configurazione guidata* a pagina 15.

Installazione dal sito Web

Quando si installa Wireless Home Network Security dal sito Web, è necessario salvare il file di installazione. Questo file viene utilizzato per installare Wireless Home Network Security su altri computer.

1. Visitare il sito Web McAfee e fare clic su **Account**.

2 Se richiesto, immettere la password e l'indirizzo di posta elettronica di sottoscrizione, quindi fare clic su **Accesso** per aprire la pagina **Informazioni sull'account**.

3 Individuare il prodotto nell'elenco dei prodotti e fare clic su **Salva oggetto con nome...** Il file di installazione è salvato sul computer.

Installazione dal file di installazione

Se è stato scaricato il pacchetto di installazione (anziché disporre di un CD), è necessario installare il software su tutti i computer senza fili. Dopo che la rete è protetta, i computer senza fili non possono connettersi alla rete senza immettere la chiave. Effettuare una delle seguenti operazioni:

- Prima di proteggere la rete, scaricare il pacchetto di installazione su ogni computer senza fili.
- Copiare il file di installazione su un supporto di memorizzazione USB o un CD scrivibile e installare il software su altri computer senza fili.
- Se la rete è già protetta, collegare un cavo al router per scaricare il file. È inoltre possibile fare clic su **Visualizza chiave di rete** per visualizzare la chiave corrente e connettersi alla rete senza fili mediante tale chiave.

Dopo aver installato Wireless Home Network Security su tutti i computer senza fili, attenersi alle istruzioni sullo schermo. Fare clic su **Fine** per visualizzare la Configurazione guidata. Andare a *Utilizzo della configurazione guidata* a pagina 15.

Utilizzo della configurazione guidata

La configurazione guidata consente di:

- Proteggere la rete da uno dei computer senza fili. Per ulteriori informazioni, vedere *Protezione delle reti senza fili* a pagina 24.

  Se Wireless Home Network Security non può determinare il corretto router o access point da proteggere, viene chiesto di riprovare o annullare. Provare ad avvicinarsi al router o all'access point che si sta proteggendo e fare clic su **Riprova**.

- Aggiungersi a una rete protetta (questo passaggio non è necessario se è presente soltanto un computer senza fili). Per ulteriori informazioni, vedere *Gestione delle reti senza fili* a pagina 18.
- Connettersi a una rete. Per ulteriori informazioni, vedere *Connessione a una rete* a pagina 19.

Se l'adattatore senza fili non viene rilevato oppure il router o l'access point senza fili non è acceso, si riceverà un avviso.

Utilizzo della pagina Riepilogo

Per visualizzare lo stato della connessione, fare clic con il pulsante destro sull'icona McAfee (M), scegliere **Wireless Network Security**, quindi selezionare **Riepilogo**. Verrà visualizzata la pagina Riepilogo (Figura 2-1).



Figura 2-1. Pagina Riepilogo

Visualizzazione della connessione

Il riquadro Connessione visualizza lo stato della connessione. Se si desidera eseguire una ricerca della connessione senza fili, fare clic su **Ricerca protezione**.

- Stato: indica se la connessione è attiva o meno. Se la connessione è attiva, verrà visualizzato il nome della rete.
- Protezione: indica la modalità di protezione della rete.
- Velocità: indica la velocità della connessione dalla scheda d'interfaccia di rete (NIC o Network Interface Card).
- Durata: indica la durata della connessione alla rete specifica.
- Potenza del segnale: indica la potenza della connessione senza fili.

Visualizzazione della rete senza fili protetta

Il riquadro Rete senza fili protetta fornisce informazioni sulla rete.

- Connessioni di oggi: indica quante volte gli utenti si sono connessi alla rete nella giornata corrente.
- Rotazioni chiave di oggi: indica quante volte la chiave è stata rotata nella giornata corrente, includendo il tempo trascorso da quando la chiave è stata rotata l'ultima volta.
- Rotazione della chiave sospesa: indica che la rotazione della chiave sulla rete è sospesa. Per riprendere la rotazione della chiave e garantire che tutta la rete sia completamente protetta dagli hacker, fare clic su **Riprendi rotazione chiave**.
- Computer protetti questo mese corrente: indica il numero dei computer protetti nel mese corrente.
- Computer: se si è connessi a una rete protetta, indica tutti i computer sulla rete e l'ultima connessione di ciascun computer.

  : indica che il computer è connesso.

  : indica che il computer può riconnettersi senza aggiungersi alla rete.

  : indica che il computer non è connesso. È necessario aggiungere nuovamente il computer alla rete perché la chiave è stata aggiornata.

Fare clic su **Visualizza eventi di rete** per visualizzare gli eventi della rete. Vedere *Visualizzazione di eventi* a pagina 20.

Fare clic su **Visualizza chiave corrente** per visualizzare la chiave.

Se si sta effettuando la connessione di dispositivi senza fili non supportati da Wireless Home Network Security (ad esempio, la connessione alla rete di un palmare senza fili), attenersi alla seguente procedura.

1. Nella schermata Riepilogo, fare clic su **Visualizza chiave corrente**.
2. Annotare la chiave.
3. Fare clic su **Sospendi rotazione chiave**. La sospensione della rotazione della chiave impedisce che i dispositivi connessi manualmente alla rete vengano disconnessi.
4. Immettere la chiave nel dispositivo.

Dopo aver utilizzato questi dispositivi, fare clic su **Riprendi rotazione chiave**. Per accertarsi che la rete sia completamente protetta contro gli hacker, McAfee raccomanda di riprendere la rotazione della chiave.

Gestione delle reti senza fili

Per selezionare le reti senza fili a cui connettersi o aggiungersi, fare clic con il pulsante destro del mouse sull'icona McAfee ( ), scegliere **Wireless Network Security** e selezionare **Reti senza fili disponibili**. Verrà visualizzata la pagina Reti senza fili disponibili (Figura 2-2).

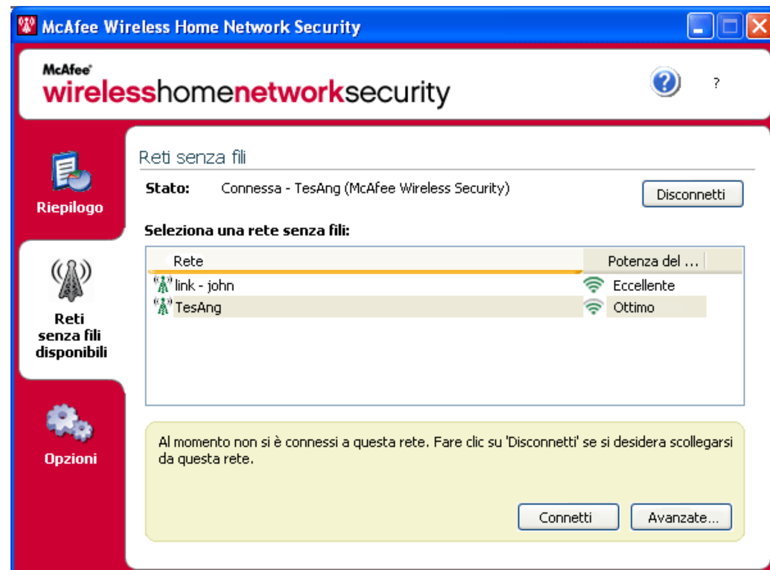


Figura 2-2. Pagina Reti senza fili disponibili

Quando si è connessi a una rete senza fili protetta, le informazioni inviate e ricevute vengono crittografate. Gli hacker non possono intercettare i dati che vengono trasmessi sulla rete protetta e non possono connettersi alla rete.

: la rete è protetta.

: la rete è protetta utilizzando la protezione WEP o WPA-PSK.

: la rete non è protetta ma è ancora possibile connettersi (non consigliato).

Connessione a una rete

Per connettersi a una rete, selezionare quella a cui si desidera connettersi e fare clic su **Connetti**. Se è stata configurata manualmente una chiave già condivisa per il router o l'access point, sarà necessario immettere anche la chiave.

Se la rete è protetta, prima di connettersi sarà necessario aggiungersi. Per aggiungersi alla rete, un utente già connesso alla rete dovrà fornire l'autorizzazione.

Quando ci si aggiunge a una rete, è possibile riconnettersi senza aggiungersi di nuovo. Inoltre è possibile autorizzare altri utenti ad aggiungersi alla rete.

Disconnessione da una rete

Per disconnettersi dalla rete alla quale si è connessi, fare clic su **Disconnetti**.

Utilizzo delle opzioni avanzate

Se si desidera utilizzare le opzioni di connessione avanzate, fare clic su **Avanzate**. Verrà visualizzata la finestra di dialogo **Impostazioni avanzate rete senza fili**. Dalla finestra di dialogo, è possibile eseguire le seguenti operazioni.

- Modificare l'ordine delle reti alle quali si ci connette automaticamente: la rete al primo posto nell'elenco è quella alla quale si è effettuato il collegamento l'ultima volta ed è quella alla quale Wireless Home Network Security tenta di connettersi per prima. Per spostare una rete, selezionarla e fare clic su **Sposta in alto** o **Sposta in basso**. Ad esempio, se ci si è allontanati dalla rete alla quale si è effettuato il collegamento l'ultima volta e la rete è ora troppo lontana e il segnale troppo debole, è possibile modificare la posizione delle reti nell'elenco in modo tale che la rete con il segnale più potente figuri al primo posto.

- Rimuovere le reti preferite: rimuovere le reti dall'elenco. Ad esempio, se ci si è connessi a una rete esterna per errore, questa viene inclusa nell'elenco. Per rimuoverla, selezionarla, quindi fare clic su **Rimuovi**.

- Modificare le proprietà di rete: se si verificano dei problemi di connessione a una rete non protetta, è possibile modificare le proprietà della rete. Notare che questa opzione è valida solo per le reti non protette. Per modificare le proprietà, selezionare una rete, quindi fare clic su **Proprietà**.

- Aggiungere reti che non trasmettono SSID: ad esempio se si prova a connettersi alla rete senza fili di un amico, ma questa non viene visualizzata nell'elenco, fare clic su **Aggiungi** e immettere le informazioni corrette. Notare che la rete aggiunta non può essere protetta da Wireless Home Network Security.

Configurazione delle opzioni

Per configurare le opzioni, fare clic con il pulsante destro del mouse sull'icona McAfee (M), scegliere **Wireless Network Security**, quindi selezionare **Opzioni**. Viene visualizzata la pagina **Opzioni** (Figura 2-3).



Figura 2-3. Pagina Opzioni

Visualizzazione di eventi

Le azioni eseguite da Wireless Home Network Security vengono memorizzate nei registri eventi. Per visualizzare tali registri, fare clic su **Visualizza eventi di rete**. Le informazioni vengono visualizzate in ordine cronologico per impostazione predefinita.

Nella casella **Eventi sulla rete**, è possibile selezionare il tipo di eventi visualizzati (tutti gli eventi vengono comunque registrati) nonché gli eventi per ciascuna rete di cui si fa parte (se si fa parte di più reti).

Quando si verifica un evento, viene visualizzato un avviso con una breve descrizione. Per ulteriori informazioni sugli avvisi, vedere *Indicazioni sugli avvisi* a pagina 26.

Configurazione delle impostazioni avanzate

Questa sezione è per gli utenti più esperti. Per configurare protezione, avvisi e altre impostazioni, fare clic su **Impostazioni avanzate**.

Quando si modifica un'impostazione, affinché le modifiche vengano applicate, fare clic su **OK**. Si noti che dopo aver fatto clic su **OK**, tutti i computer connessi temporaneamente perdono la connettività per alcuni minuti.

Configurazione delle impostazioni di protezione

Per modificare le impostazioni di protezione, utilizzare la scheda **Impostazioni protezione**.

- Nome rete senza fili protetta: nome della rete corrente protetta. Quando si modifica il nome di una rete, viene visualizzato nell'elenco **Reti senza fili disponibili** ed è necessario riconnettersi alla rete. Vedere *Gestione delle reti senza fili* a pagina 18.
- Modalità protezione: modalità di protezione corrente. Per modificare la protezione predefinita (WEP), selezionare WPA-PSK TKIP per una crittografia più efficace. Accertarsi che i router, gli access point e gli adattatori senza fili che si connettono alla rete supportino questa modalità, altrimenti non saranno in grado di connettersi. Per ulteriori informazioni sull'aggiornamento dell'adattatore, vedere *Aggiornamento dell'adattatore senza fili* a pagina 34.
- Attiva rotazione automatica chiave: per sospendere la rotazione della chiave, deselezionare questa opzione. Per modificare la frequenza della rotazione della chiave, spostare il dispositivo di scorrimento. Per ulteriori informazioni sulla rotazione della chiave, vedere *Visualizzazione della rete senza fili protetta* a pagina 17.
- Cambia nome utente o password: per motivi di sicurezza, è possibile modificare la password o il nome utente predefinito per il router o l'access point senza fili, selezionandolo e facendo clic su **Cambia nome utente o password**. Il nome utente o la password predefiniti sono quelli utilizzati quando si è effettuato l'accesso e la configurazione del router o dell'access point.

Configurazione delle impostazioni di avviso

Per modificare le impostazioni di avviso, utilizzare la scheda **Impostazioni avviso**.

Selezionare il tipo di eventi di cui si desidera essere avvisati e fare clic su **OK**. Se non si desidera essere avvisati riguardo alcuni tipi di eventi, deselezionare la casella appropriata.

Configurazione di altre impostazioni

Per modificare le altre impostazioni, utilizzare la scheda **Altre impostazioni**.

- Visualizza chiavi in testo normale: per le reti non protette da Wireless Home Network Security. Le chiavi per le reti non protette visualizzate nell'elenco **Reti senza fili disponibili** possono essere visualizzate in testo normale anziché in asterischi. Se si visualizzano le chiavi in testo normale, queste vengono eliminate per motivi di sicurezza.
- Ignora tutte le chiavi salvate: per le reti non protette da Wireless Home Network Security. Eliminare tutte le chiavi salvate. Si noti che se si eliminano queste chiavi, quando ci si connette alle reti WEP e WPA-PSK è necessario immettere di nuovo una chiave.
- Abbandona rete: per le reti protette da Wireless Home Network Security. È possibile rifiutare i diritti di accesso a una rete senza fili protetta. Ad esempio, se si desidera abbandonare una rete e si prevede di non connettersi di nuovo, selezionarla dall'elenco e fare clic su **Abbandona rete**.
- Visualizza messaggio di notifica quando si è connessi a una rete senza fili: quando viene effettuata una connessione, viene visualizzato un messaggio di notifica.

Revoca dell'accesso alla rete

Per impedire l'accesso alla rete da parte di computer che si sono aggiunti alla rete, ma che non sono correntemente connessi, attenersi alla seguente procedura:

1. Fare clic su **Revoca accesso**. Verrà visualizzata la finestra di dialogo **Revoca accesso**.
2. Fare clic su **Revoca**.

La rotazione della chiave viene ripristinata, i computer connessi al momento ricevono la nuova chiave e non vengono disconnessi. I computer non connessi al momento non ricevono la chiave aggiornata e devono nuovamente aggiungersi alla rete prima di potersi connettere.

Quando si revoca l'accesso a un computer, il computer deve riaggiungersi alla rete protetta prima che possa connettersi di nuovo. Per effettuare tale operazione è necessario che sul computer sia installato Wireless Home Network Security (vedere *Installazione di Wireless Home Network Security* a pagina 14), quindi connettersi alla rete protetta e aggiungersi di nuovo (vedere *Connessione a una rete* a pagina 19).

Ripristino delle impostazioni di protezione

Ripristinare le impostazioni di protezione solo se si riscontrano problemi con la rete senza fili. Per ulteriori informazioni, vedere *Impossibile connettersi* a pagina 34.

Per correggere le impostazioni di un router o un access point sulla rete corrente, attenersi alla seguente procedura.

1 Fare clic su **Ripristina impostazioni protezione.** Verrà visualizzata la finestra di dialogo **Ripristina**.

2 Fare clic su **Ripristina**.

3 Al termine, fare clic su **Chiudi**.

Se non è possibile stabilire una connessione con i router o gli access point della rete, verrà visualizzato un messaggio di errore. Connettersi alla rete utilizzando un cavo, quindi tentare nuovamente il ripristino. Se la password per il router o l'access point è stata modificata, verrà richiesta la nuova password.

Protezione di altri computer

Per ottenere ulteriori informazioni su come proteggere altri computer e farli accedere alla rete protetta, fare clic su **Proteggi un altro computer**.

Per proteggere un altro computer, attenersi alla seguente procedura.

1 Installare McAfee Wireless Home Network Security sul computer che si desidera proteggere.

2 Dal computer che si sta proteggendo, fare clic con il pulsante destro del mouse sull'icona McAfee ( ), scegliere **Wireless Network Security**, quindi selezionare **Reti senza fili disponibili**. Verrà visualizzata la pagina Reti senza fili disponibili.

3 Selezionare una rete protetta a cui aggiungersi, quindi fare clic su **Connetti**. Per aggiungersi alla rete, è necessario ricevere l'autorizzazione da un utente già connesso alla rete.

   Quando ci si aggiunge a una rete, è possibile riconnettersi senza aggiungersi di nuovo. Inoltre è possibile autorizzare altri utenti ad aggiungersi alla rete.

4 Fare clic su **OK** nella finestra di dialogo di conferma.

Se si sta effettuando la connessione di dispositivi senza fili non supportati da Wireless Home Network Security (ad esempio, la connessione alla rete di un palmare senza fili), attenersi alla seguente procedura.

1 Nella schermata Riepilogo, fare clic su **Visualizza chiave corrente**.

2 Annotare la chiave.

3 Fare clic su **Sospendi rotazione chiave**. La sospensione della rotazione della chiave impedisce che i dispositivi connessi manualmente alla rete vengano disconnessi.

4 Immettere la chiave nel dispositivo.

Dopo aver utilizzato questi dispositivi, fare clic su **Riprendi rotazione chiave**. Per accertarsi che la rete sia completamente protetta contro gli hacker, McAfee raccomanda di riprendere la rotazione della chiave.

Rotazione delle chiavi

Per effettuare la rotazione della chiave di protezione per la rete, fare clic su **Ruota manualmente la chiave di protezione**.

Protezione delle reti senza fili

Per proteggere un router o un access point, attenersi alla seguente procedura.

1 Fare clic su **Proteggi router/AP senza fili**. Verrà visualizzata la finestra di dialogo **Proteggi rete senza fili**. Se il router o l'access point non viene visualizzato nell'elenco, fare clic su **Aggiorna**.

2 Selezionare il router o l'access point che si desidera proteggere, quindi fare clic su **Proteggi**.

Rimozione della protezione dalle reti senza fili

È necessario essere connessi al router o all'access point senza fili dal quale si desidera rimuovere la protezione.

Per rimuovere la protezione di un router o un access point, attenersi alla seguente procedura.

1 Fare clic su **Rimuovi protezione router/AP senza fili**. Verrà visualizzata la finestra di dialogo **Rimuovi protezione rete senza fili**. Se il router o l'access point non viene visualizzato nell'elenco, fare clic su **Aggiorna**.

2 Selezionare il router o l'access point dal quale si desidera rimuovere la protezione, quindi fare clic su **Rimuovi protezione**.

Aggiornamento di Wireless Home Network Security

Quando si è connessi a Internet, Wireless Home Network Security verifica la disponibilità di aggiornamenti ogni quattro ore, quindi scarica e installa automaticamente gli aggiornamenti settimanali senza interrompere le operazioni in corso. Questi aggiornamenti hanno un impatto minimo sulle prestazioni del sistema durante il download.

In caso di aggiornamento di un prodotto, viene visualizzato un avviso. Quando si riceve l'avviso, è possibile aggiornare Wireless Home Network Security.

Verifica automatica della disponibilità di aggiornamenti

McAfee SecurityCenter è configurato automaticamente per verificare gli aggiornamenti di tutti i servizi McAfee ogni quattro ore quando si è connessi a Internet e per notificare tali aggiornamenti con avvisi e segnali acustici. Per impostazione predefinita, SecurityCenter scarica e installa automaticamente tutti gli aggiornamenti disponibili.

NOTA
In alcuni casi, viene richiesto di riavviare il computer per completare l'aggiornamento. Salvare le modifiche effettuate e chiudere tutte le applicazioni in esecuzione prima di riavviare.

Verifica manuale della disponibilità di aggiornamenti

Oltre alla verifica automatica durante la connessione a Internet, è possibile verificare manualmente la disponibilità di aggiornamenti in qualsiasi momento.

Per verificare manualmente la disponibilità di aggiornamenti di Wireless Home Network Security, attenersi alla seguente procedura:

1. Assicurarsi che il computer sia connesso a Internet.
2. Fare clic con il pulsante destro del mouse sull'icona McAfee, quindi scegliere **Aggiornamenti**. Verrà visualizzata la finestra di dialogo **Aggiornamenti di SecurityCenter**.
3. Fare clic su **Controlla**.

   Se è disponibile un aggiornamento, verrà visualizzata la finestra di dialogo **McAfee SecurityCenter**. Fare clic su **Aggiorna** per continuare.

   Se non è disponibile alcun aggiornamento, verrà visualizzata una finestra di dialogo per segnalare che Wireless Home Network Security è aggiornato. Fare clic su **OK** per chiudere la finestra di dialogo.

4 Se richiesto, accedere al sito Web. La **procedura guidata di aggiornamento** consente di installare automaticamente l'aggiornamento.

5 Al termine dell'installazione dell'aggiornamento fare clic su **Fine**.

NOTA
In alcuni casi, viene richiesto di riavviare il computer per completare l'aggiornamento. Salvare le modifiche effettuate e chiudere tutte le applicazioni in esecuzione prima di riavviare.

Indicazioni sugli avvisi

Gli avvisi vengono visualizzati quando si verifica un evento e notificano le modifiche apportate alla rete.

Accesso revocato

Un utente ha aggiornato la chiave di rete. Per ulteriori informazioni, vedere *Revoca dell'accesso alla rete* a pagina 22.

Chiave di protezione rotata

La chiave di protezione per la rete è stata rotata. McAfee Wireless Home Network Security effettua la rotazione automatica della chiave di crittografia della rete, rendendo più difficile agli hacker l'intercettazione dei dati o la connessione alla rete.

Computer connesso

Un utente si è connesso alla rete. Per ulteriori informazioni, vedere *Connessione a una rete* a pagina 19.

Computer protetto

Un utente che dispone dell'accesso alla rete protetta ha autorizzato un altro utente all'accesso. Esempio: 'Lance' ha autorizzato l'accesso a 'Mercks' e ora possono utilizzare entrambi la rete senza fili 'CoppiWAP'.

Computer sconnesso

Un utente si è sconnesso dalla rete. Per ulteriori informazioni, vedere *Disconnessione da una rete* a pagina 19.

Configurazione di rete modificata

Un utente ha modificato la modalità di protezione per la rete. Per ulteriori informazioni, vedere *Configurazione delle impostazioni di protezione* a pagina 21.

Frequenza della rotazione della chiave di protezione modificata

La frequenza della rotazione della chiave di protezione per la rete è stata modificata. McAfee Wireless Home Network Security effettua la rotazione automatica della chiave di crittografia della rete, rendendo più difficile agli hacker l'intercettazione dei dati o la connessione alla rete.

Impostazioni di rete modificate

Un utente sta per modificare le impostazioni di protezione della rete. La connessione verrà interrotta temporaneamente durante tale operazione. La modifica potrebbe interessare una o più delle seguenti impostazioni:

- Nome di rete
- Modalità protezione
- Frequenza della chiave sospesa
- Stato della rotazione automatica della chiave

Password modificata

Un utente ha modificato il nome utente o la password su un router o access point sulla rete. Per ulteriori informazioni, vedere *Configurazione delle impostazioni di protezione* a pagina 21.

Rete ridenominata

Un utente ha ridenominato la rete ed è necessario connettersi di nuovo. Per ulteriori informazioni, vedere *Connessione a una rete* a pagina 19.

Rete ripristinata

Un utente ha tentato di ripristinare la rete perché si riscontravano problemi di connessione.

Rotazione della chiave non riuscita

La rotazione della chiave non è riuscita perché:

- Le informazioni di accesso per il router o l'access point sono state modificate. Se si dispone delle informazioni di accesso, vedere *Ripristino delle impostazioni di protezione* a pagina 23.
- La versione firmware del router o dell'access point è stata modificata con una versione che non è supportata. Per ulteriori informazioni, vedere *Impossibile connettersi* a pagina 34.
- Il router o l'access point non è disponibile. Accertarsi che il router o l'access point sia attivato e che sia connesso alla rete.
- Errore di duplicazione amministratore. Per ulteriori informazioni, vedere *Errore di amministratore duplicato* a pagina 31.

Se si riscontrano problemi di connessione con questa rete, vedere *Ripristino delle impostazioni di protezione* a pagina 23.

Rotazione della chiave ripresa

Un utente ha ripreso la rotazione della chiave. La rotazione della chiave impedisce agli hacker di accedere alla rete.

Rotazione della chiave sospesa

Un utente ha sospeso la rotazione della chiave. Per accertarsi che la rete sia completamente protetta contro gli hacker, McAfee raccomanda di riprendere la rotazione della chiave.

Router o access point senza fili non protetto

Un router o access point senza fili è stato rimosso dalla rete. Per ulteriori informazioni, vedere *Rimozione della protezione dalle reti senza fili* a pagina 24.

Router o access point senza fili protetto

Un router o access point senza fili è stato protetto sulla rete. Per ulteriori informazioni, vedere *Protezione delle reti senza fili* a pagina 24.

Risoluzione dei problemi

Questo capitolo descrive le procedure per la risoluzione dei problemi di McAfee Wireless Home Network Security e dispositivi di terzi.

Installazione

Questa sezione spiega come risolvere problemi di installazione.

Su quali computer installare questo software

Installare McAfee Wireless Home Network Security su ciascun computer senza fili nella rete (a differenza di altre applicazioni McAfee, è possibile installare questo software su diversi computer).

È possibile (ma non necessario) installarlo su computer che non dispongono di adattatori senza fili, ma il software non sarà attivo su tali computer perché non necessitano di protezione senza fili. Per proteggere la rete è necessario proteggere il router o l'access point (vedere *Protezione delle reti senza fili* a pagina 24) da uno dei computer senza fili.

Adattatore senza fili non rilevato

Se l'adattatore senza fili non viene rilevato al momento dell'installazione e dell'attivazione, riavviare il computer. Se l'adattatore continua a non essere rilevato dopo aver riavviato il computer, attenersi alla seguente procedura.

1 Aprire la finestra di dialogo **Proprietà connessione senza fili**.

2 Deselezionare la casella **Filtro MWL**, quindi selezionarla.

3 Fare clic su **OK**.

Se questo non funziona, l'adattatore senza fili potrebbe non essere supportato. Aggiornare l'adattatore o acquistarne uno nuovo. Per visualizzare un elenco di adattatori supportati, passare a http://www.mcafee.com/it/router. Per aggiornare l'adattatore, vedere *Aggiornamento dell'adattatore senza fili* a pagina 34.

Più adattatori senza fili

Se un messaggio di errore conferma che sono stati installati più adattatori senza fili, è necessario disattivarne o scollegarne uno. Wireless Home Network Security funziona esclusivamente con un solo adattatore senza fili.

Impossibile effettuare il download sui computer senza fili perché la rete è già protetta

Se si dispone di un CD, installare McAfee Wireless Home Network Security dal CD su tutti i computer senza fili.

Se è stato installato il software su uno dei computer senza fili e la rete è stata protetta prima di installare il software su tutti gli altri computer senza fili, sono disponibili le seguenti opzioni.

- Rimuovere la protezione dalla rete (vedere *Rimozione della protezione dalle reti senza fili* a pagina 24). Quindi, scaricare il software e installarlo su tutti i computer senza fili. Proteggere di nuovo la rete (vedere *Protezione delle reti senza fili* a pagina 24).
- Visualizzare la chiave di rete (vedere *Visualizzazione della rete senza fili protetta* a pagina 17). Quindi, immettere la chiave sul computer senza fili per connettersi alla rete. Scaricare e installare il software, quindi aggiungersi alla rete dal computer senza fili (vedere *Protezione di altri computer* a pagina 23).
- Scaricare l'eseguibile sul computer già connesso alla rete e salvarlo su un dispositivo di memorizzazione USB o masterizzarlo su un CD in modo da poterlo installare su altri computer.

Protezione o configurazione della rete

Questa sezione spiega come risolvere i problemi di protezione e configurazione di una rete.

Router o access point non supportato

Se un errore informa che il router o l'access point senza fili non è supportato, McAfee Wireless Home Network Security non sarà stato in grado di configurare il dispositivo perché non l'ha rilevato o trovato.

Verificare di disporre della versione più recente di Wireless Home Network Security richiedendo un aggiornamento (McAfee aggiunge costantemente supporto per i nuovi router e access point). Se il router o l'access point viene visualizzato nell'elenco all'indirizzo http://www.mcafee.com/it/router e si riceve comunque questo errore, si stanno verificando errori di comunicazione tra il computer e il router o l'access point. Vedere *Impossibile connettersi* a pagina 34 prima di proteggere di nuovo la rete.

Aggiornamento del firmware del router o dell'access point

Se un errore informa che il firmware del router o dell'access point senza fili non è supportato, il dispositivo in uso è supportato ma la revisione firmware del dispositivo non lo è. Verificare di disporre della versione più recente di Wireless Home Network Security richiedendo un aggiornamento (McAfee aggiunge costantemente supporto per le nuove revisioni firmware).

Se si dispone della versione più recente di Wireless Home Network Security, fare riferimento al sito Web del produttore o all'azienda di supporto per il router o l'access point e installare una nuova versione del firmware elencata in http://www.mcafee.com/it/router.

Errore di amministratore duplicato

Dopo aver configurato il router o l'access point, è necessario disconnettersi dall'interfaccia di amministrazione. A volte, in caso di mancata disconnessione, il router o l'access point si comporta come se fosse in fase di configurazione tramite un altro computer. In tal caso viene visualizzato un messaggio di errore.

Se non è possibile disconnettersi, scollegare l'alimentazione dal router o dall'access point, quindi ricollegarla.

La rete risulta non sicura

Se la rete risulta non sicura, non è protetta. È necessario proteggerla (vedere *Protezione delle reti senza fili* a pagina 24) per renderla sicura. È opportuno considerare che McAfee Wireless Home Network Security funziona soltanto con router e access point compatibili (vedere http://www.mcafee.com/it/router).

Impossibile ripristinare

Se non è possibile eseguire il ripristino, provare quanto riportato di seguito. Ciascuna delle seguenti procedure è indipendente.

- Connettersi alla rete utilizzando un cavo, quindi tentare nuovamente il ripristino.
- Scollegare l'alimentazione dal router o dall'access point, ricollegarlo di nuovo, quindi tentare la connessione.
- Ripristinare le impostazioni predefinite del router o dell'access point, quindi eseguire il ripristino.
- Utilizzare le opzioni avanzate, disconnettere tutti i computer dalla rete e ripristinare le impostazioni predefinite del router o dell'access point senza fili, quindi attivare la protezione.

Connessione di computer a una rete

Questa sezione spiega come risolvere i problemi di connessione dei computer a una rete.

In attesa di autorizzazione

Se si tenta di aggiungersi a una rete protetta e il computer resta nella modalità di attesa dell'autorizzazione, verificare quanto segue.

- Un computer senza fili che dispone già dell'accesso alla rete è acceso e connesso alla rete.
- È presente qualcuno per concedere l'accesso al computer quando viene visualizzato.
- I computer si trovano nel raggio di azione senza fili reciproco.

Se **Consenti accesso** non viene visualizzato sul computer che già dispone dell'accesso alla rete, provare a concedere l'accesso da un altro computer.

Se non sono disponibili altri computer, rimuovere la protezione della rete dal computer che già dispone dell'accesso e proteggere la rete dal computer che non disponeva dell'accesso. Quindi, aggiungersi alla rete dal computer che inizialmente proteggeva la rete.

Autorizzazione dell'accesso a un computer sconosciuto

Quando si riceve una richiesta di autorizzazione di accesso da un computer sconosciuto, verificarne l'identità. Potrebbe trattarsi di un tentativo di accesso illegittimo alla rete.

Connessione a una rete o a Internet

Questa sezione spiega come risolvere i problemi di connessione a una rete o a Internet.

Connessione a Internet non valida

Se non è possibile connettersi, tentare di accedere alla rete utilizzando un cavo, quindi connettersi a Internet. Se ancora non è possibile connettersi, verificare quanto segue:

- Il modem è acceso
- Le impostazioni PPPoE (vedere il *Glossario* a pagina 38) sono corrette
- La linea DSL o via cavo è attiva

I problemi di connettività, quali la velocità e la potenza del segnale, possono essere causati anche da interferenze di altri dispositivi senza fili. Provare a modificare il canale del telefono cordless, eliminare le possibili fonti di interferenza o cambiare la posizione del router, access point o computer senza fili.

Interruzione momentanea della connessione

Quando la connessione si interrompe temporaneamente (ad esempio, durante un gioco online), la rotazione della chiave potrebbe provocare brevi ritardi della rete. Sospendere momentaneamente la rotazione della chiave. Si consiglia di riprendere la rotazione della chiave appena si è in grado di garantire la completa protezione della rete dagli hacker.

Perdita della connessione sui dispositivi (diversi dal computer)

Se la connessione di alcuni dispositivi viene interrotta durante l'utilizzo di McAfee Wireless Home Network Security, sospendere la rotazione della chiave.

Richiesta di immissione della chiave WEP o WPA

Se è necessario immettere una chiave WEP o WPA per collegarsi alla rete, probabilmente il software non è stato installato sul computer. Per il corretto funzionamento, è necessario che Wireless Home Network Security sia installato su ciascun computer senza fili nella rete. Vedere *Protezione o configurazione della rete* a pagina 30.

Impossibile connettersi

Se ancora non è possibile connettersi, provare quanto riportato di seguito. Ciascuna delle seguenti procedure è indipendente.

- Se non si è collegati a una rete protetta, verificare di disporre della chiave corretta e immetterla nuovamente.
- Disconnettere l'adattatore senza fili, quindi connetterlo nuovamente oppure disattivarlo e riattivarlo nuovamente.
- Spegnere il router o l'access point, accenderlo nuovamente, quindi tentare la connessione.
- Verificare che il router o l'access point senza fili sia connesso e ripristinare le impostazioni di protezione (vedere *Ripristino delle impostazioni di protezione* a pagina 23).

  Se non è possibile eseguire il ripristino, vedere *Impossibile ripristinare* a pagina 31.
- Riavviare il computer.
- Aggiornare l'adattatore senza fili o acquistarne uno nuovo. Per aggiornare l'adattatore, vedere *Aggiornamento dell'adattatore senza fili* a pagina 34. Ad esempio, la rete potrebbe utilizzare la protezione WPA-PSK TKIP e l'adattatore senza fili potrebbe non supportare la modalità di protezione della rete (le reti visualizzano WEP, anche se sono state impostate su WPA).
- Se non è possibile connettersi dopo aver aggiornato il router o l'access point senza fili, potrebbe essere stato eseguito l'aggiornamento a una versione non supportata. Verificare che il router o l'access point sia supportato. Se non fosse supportato, effettuare il downgrade a una versione supportata oppure attendere la disponibilità di un aggiornamento di Wireless Home Network Security.

Aggiornamento dell'adattatore senza fili

Per aggiornare l'adattatore, attenersi alla seguente procedura.

1. Sul desktop, fare clic su **Start**, scegliere **Impostazioni**, quindi **Pannello di controllo**.
2. Fare doppio clic sull'icona **Sistema**. Verrà visualizzata la finestra di dialogo **Proprietà di sistema**.
3. Selezionare la scheda **Hardware**, quindi fare clic su **Gestione periferiche**.
4. Nell'elenco **Gestione periferiche**, fare doppio clic sull'adattatore.
5. Selezionare la scheda **Driver** e verificare il driver a disposizione.

6 Visitare il sito Web del produttore dell'adattatore e verificare la disponibilità di un aggiornamento. I driver si trovano solitamente nella sezione Supporto o Download.

7 Se è disponibile l'aggiornamento di un driver, seguire le istruzioni riportate sul sito Web per effettuarne il download.

8 Tornare alla scheda **Driver**, quindi fare clic su **Aggiorna driver**. Verrà visualizzata una procedura guidata di Windows.

9 Seguire le istruzioni riportate sullo schermo.

Livello del segnale debole

Se la connessione si interrompe o è lenta, il livello del segnale potrebbe non essere abbastanza potente. Per migliorare il segnale, provare quanto riportato di seguito.

- Verificare che i dispositivi senza fili non siano bloccati da oggetti metallici quali bruciatori, condutture o apparecchi di grandi dimensioni. I segnali senza fili non passano attraverso questi oggetti.
- Se il segnale deve attraversare delle pareti, accertarsi che non debba essere trasmesso attraverso un angolo vuoto, più tempo il segnale impiega all'interno della parete, più si indebolisce.
- Se il router o l'access point senza fili dispone di più antenne, provare ad orientare le due antenne perpendicolarmente l'una all'altra (ad esempio, una verticale e l'altra orizzontale ad angolo di 90°).
- Alcuni produttori dispongono di antenne ad alta ricezione. Le antenne direzionali offrono un raggio d'azione più lungo, mentre le antenne omnidirezionali offrono maggiore versatilità. Consultare le istruzioni di installazione del produttore per effettuare l'installazione dell'antenna.

Se questa procedura non riesce, aggiungere un access point alla rete più vicino al computer al quale si sta tentando di connettersi. Se si configura il secondo AP con lo stesso nome di rete (SSID) e con un canale differente, l'adattatore individuerà automaticamente il segnale più potente e si collegherà attraverso l'AP appropriato.

Windows non è in grado di configurare la connessione senza fili

Ignorare eventuali messaggi che informano che Windows non è in grado di configurare la connessione senza fili. Utilizzare Wireless Home Network Security per connettersi a reti senza fili e per configurarle. Nella finestra di dialogo di Windows **Proprietà connessione senza fili**, nella scheda **Reti senza fili**, verificare che la casella **Usa Windows per configurare le impostazioni della rete senza fili** non sia selezionata.

Windows non visualizza alcuna connessione

Se si stabilisce una connessione, ignorare l'icona di rete di Windows in caso presenti una X (nessuna connessione). Si è stabilita una buona connessione.

Altri problemi

Questa sezione spiega come risolvere altri tipi di problemi.

Nome di rete differente durante l'utilizzo di altri programmi

Se il nome della rete è diverso quando viene visualizzato tramite altri programmi (ad esempio, _SafeAaf è parte del nome) non c'è da preoccuparsi. Wireless Home Network Security contrassegna le reti con un codice quando sono protette.

Problemi di configurazione dei router o degli access point senza fili

Se si verifica un errore durante la configurazione del router o dell'access point o durante l'aggiunta di più router sulla rete, verificare che tutti i router o gli access point presentino un indirizzo IP distinto.

Se il nome del router o dell'access point senza fili viene visualizzato nella finestra di dialogo **Proteggi router o access point**, ma si verifica un errore durante la configurazione, verificare che il router o l'access point sia supportato. Per visualizzare un elenco di router o access point supportati, passare a http://www.mcafee.com/it/router.

Se il router o l'access point è configurato, ma non sembra essere sulla rete corretta (ad esempio, non vengono visualizzati altri computer collegati alla LAN), verificare di aver configurato il router o l'access point appropriato. Scollegare l'alimentazione dal router o dall'access point e verificare che la connessione venga interrotta. Se viene configurato il router o l'access point errato, rimuovere la protezione e applicarla al router o all'access point corretto.

Se è impossibile configurare o aggiungere il router o l'access point, ma si è sicuri che sia supportato, alcune modifiche apportate potrebbero impedirne la corretta configurazione.

- Seguire le indicazioni del produttore per configurare il router o l'access point senza fili per il DHCP o per configurare il corretto indirizzo IP. In alcuni casi, il produttore fornisce uno strumento di configurazione.

- Ripristinare le impostazioni di fabbrica del router o dell'access point e provare nuovamente a ripristinare la rete. La porta di amministrazione potrebbe essere stata modificata oppure l'amministrazione senza fili potrebbe essere stata disattivata. Verificare che venga utilizzata la configurazione predefinita e che la configurazione senza fili sia attivata. Un'altra possibilità è che l'amministrazione http sia disattivata. In questo caso, verificare che l'amministrazione http sia attivata.
- Se il router o l'access point senza fili non viene visualizzato nell'elenco dei router o degli access point senza fili che è possibile proteggere o ai quali è possibile connettersi, attivare la trasmissione SSID e verificare che il router o l'access point sia attivato.
- In caso si venga disconnessi o sia impossibile stabilire una connessione, i filtri MAC potrebbero essere attivati. Disattivare i filtri MAC.
- Se non è possibile eseguire operazioni di rete (ad esempio, condividere file o eseguire la stampa su stampanti condivise) tra due computer connessi alla rete senza fili, verificare di non aver attivato l'isolamento dell'access point. L'isolamento dell'access point impedisce che i computer senza fili vengano connessi tra di loro tramite la rete.

Sostituzione di computer

Se il computer che gestisce la protezione della rete viene sostituito e non esistono altri computer che dispongono dell'accesso (è impossibile accedere alla rete), ripristinare le impostazioni di fabbrica del router o dell'access point senza fili e applicare di nuovo la protezione sulla rete.

Software non funzionante in seguito all'aggiornamento dei sistemi operativi

Se Wireless Home Network Security non funziona dopo aver aggiornato i sistemi operativi, disinstallare e installare nuovamente il programma.

Glossario

802.11

Insieme di standard IEEE per la tecnologia LAN senza fili. 802.11 specifica un'interfaccia over-the-air tra un client senza fili e una stazione di base o tra due client senza fili. Diverse specifiche di 802.11 includono 802.11a, uno standard per una connessione di rete fino a 54 Mbps nella banda da 5 Ghz, 802.11b, uno standard per una connessione di rete fino a 11 Mbps nella banda da 2,4 Ghz, 802.11g, uno standard per una connessione di rete fino a 54 Mbps nella banda da 2,4 Ghz e 802.11i, una suite di standard di protezione per tutte le Ethernet senza fili.

802.11a

Estensione di 802.11 che si applica alle LAN senza fili e invia dati fino a 54 Mbps nella banda da 5 GHz. Nonostante la velocità di trasmissione sia superiore che in 802.11 b, la distanza coperta è di gran lunga inferiore.

802.11b

Estensione di 802.11 che si applica alle LAN senza fili e fornisce la trasmissione da 11 Mbps nella banda da 2,4 GHz. 802.11b è attualmente considerato lo standard senza fili.

802.11g

Estensione di 802.11 che si applica alle LAN senza fili e fornisce fino a 54 Mbps nella banda da 2,4 GHz.

802.1x

Non supportato da Wireless Home Network Security. Si tratta di uno standard IEEE per l'autenticazione su reti cablate e senza fili, ma viene utilizzato soprattutto insieme alla connessione di rete senza fili 802.11. Questo standard fornisce un'autenticazione reciproca e potente tra un client e un server di autenticazione. Inoltre, 802.1x può fornire chiavi WEP dinamiche utente per utente e per sessione, diminuendo il carico amministrativo e i rischi per la protezione legati alle chiavi WEP statiche.

A

Access Point (AP)

Dispositivo di rete che consente ai client 802.11 di connettersi a una rete locale (LAN). Gli AP estendono la gamma fisica di servizi per un utente senza fili. Talvolta sono denominati router senza fili.

Access point pericoloso

Access point di cui un'azienda non autorizza il funzionamento. Questo tipo di access point spesso non è conforme ai criteri di protezione della LAN senza fili (WLAN). Un access point pericoloso attiva un'interfaccia non protetta e aperta alla rete aziendale dall'esterno della struttura fisicamente controllata.

All'interno di una WLAN correttamente protetta, gli access point pericolosi sono più dannosi degli utenti pericolosi. Se sono attivi dei meccanismi di autenticazione efficaci, è probabile che gli utenti non autorizzati che tentano l'accesso a una WLAN non riescano a raggiungere le preziose risorse aziendali. Maggiori problemi sorgono, tuttavia, quando un impiegato o un hacker si collega a un access point pericoloso. Questo, infatti, consente l'accesso alla rete aziendale a chiunque disponga di un dispositivo dotato di 802.11, consentendogli di avvicinarsi a importanti risorse.

Adattatore senza fili

Contiene i circuiti che consentono a un computer o altri dispositivi di comunicare con un router senza fili (collegamento a una rete senza fili). Gli adattatori senza fili possono essere incorporati nei circuiti principali di un dispositivo hardware oppure essere costituiti da un componente aggiuntivo a parte da inserire nel dispositivo mediante un'apposita porta.

Attacco di forza bruta

Noto anche come brute force cracking, si tratta di un metodo di prova ed errore utilizzato da applicazioni per decodificare dati crittografati come le password, mediante uno sforzo notevole (mediante la forza bruta) piuttosto che impiegando strategie intellettuali. Proprio come un criminale potrebbe forzare una cassaforte o aprirla tentando diverse combinazioni possibili, un'applicazione che utilizza la forza bruta procede attraverso tutte le possibili combinazioni dei caratteri consentiti in sequenza. L'uso della forza bruta è considerato un approccio infallibile anche se piuttosto lungo.

Attacco di tipo Dictionary

Tipo di attacco che consiste nei tentativi di individuare le password utilizzando una gran quantità di parole contenute in un elenco. Gli hacker non tentano manualmente tutte le combinazioni, ma dispongono di strumenti che tentano automaticamente di identificare una determinata password.

Attacco di tipo Man-in-the-Middle

L'hacker intercetta i messaggi in uno scambio di chiavi pubbliche e li ritrasmette sostituendone la chiave pubblica con quella richiesta, in modo che le due parti originarie risultino ancora in comunicazione diretta tra loro. L'hacker utilizza un programma che al client sembra il server e al server sembra il client. L'attacco può essere utilizzato semplicemente per ottenere accesso ai messaggi o per consentire all'hacker di modificarli prima di trasmetterli di nuovo. Il termine deriva da un gioco in cui i partecipanti tentano di lanciarsi una palla mentre un altro giocatore nel mezzo tenta di afferrarla.

Autenticazione

Processo di identificazione di un individuo, di solito basato su un nome utente e una password. L'autenticazione verifica l'autenticità dell'identità dichiarata dall'utente, ma non fornisce alcun dato sui suoi diritti di accesso.

B

C

Chiave

Serie di lettere e/o numeri utilizzata da due dispositivi per autenticarne la comunicazione. Entrambi i dispositivi devono disporre di una chiave. Vedere anche WEP e WPA-PSK.

Client

Applicazione eseguita su PC o workstation e risiedente su un server per l'esecuzione di alcune operazioni. Ad esempio, un client di posta elettronica è un'applicazione che consente l'invio e la ricezione di messaggi di posta elettronica.

Crittografia

Conversione dei dati in un codice segreto. La crittografia è il modo più efficace per ottenere una protezione dei dati. Per leggere un file crittografato, è necessario disporre di una chiave o una password segreta che ne consenti la codifica. I dati non crittografati sono detti testo normale; i dati crittografati sono detti testo in codice.

D

E

ESS (Extended Service Set)

Insieme di una o più reti che formano un'unica sottorete.

F

Firewall

Sistema progettato per impedire l'accesso non autorizzato a o da una rete privata. I firewall possono essere implementati sia nell'hardware che nel software o con una combinazione di entrambi. I firewall vengono utilizzati di frequente per impedire a utenti Internet non autorizzati di accedere a reti private connesse a Internet, specialmente a una intranet. Tutti i messaggi in entrata o in uscita da una intranet passano attraverso il firewall. Il firewall esamina tutti i messaggi e blocca quelli sono conformi ai criteri di protezione specificati. È considerato la prima linea di difesa nella protezione delle informazioni private. Per una maggiore protezione, è possibile crittografare i dati.

G

Gateway integrato

Dispositivo che combina le funzioni di access point (AP), router e firewall. Alcuni dispositivi possono persino includere funzionalità avanzate di protezione e bridging.

H

Hotspot

Specifico luogo geografico in cui un access point (AP) fornisce servizi pubblici di rete a banda larga senza fili a visitatori mobili attraverso una rete senza fili. Gli hotspot si trovano spesso in luoghi particolarmente affollati come gli aeroporti, le stazioni ferroviarie, le librerie, i porti marittimi, i centri congressuali e gli alberghi. Di solito dispongono di una portata di accesso limitata.

I

Indirizzo IP

Identificativo di un computer o un dispositivo su una rete TCP/IP. Le reti che utilizzano il protocollo TCP/IP instradano i messaggi in base all'indirizzo IP della destinazione. L'indirizzo IP presenta il formato di un indirizzo dinamico a 32 bit espresso con quattro numeri separati da punti. Ogni numero può essere compreso tra zero e 255. Ad esempio, 192.168.1.100 può essere un indirizzo IP.

Indirizzo MAC (Media Access Control Address)

Indirizzo di livello basso assegnato al dispositivo fisico che accede alla rete.

J

K

L

LAN (Local Area Network)

Rete di computer che si estende in un'area relativamente ridotta. Molte LAN sono ristrette a un solo edificio o gruppo di edifici. Tuttavia, una LAN può essere connessa ad altre LAN a qualunque distanza tramite telefono e onde radio. Un sistema di LAN connesse in questo modo è detto WAN (Wide-Area Network).

Molte LAN si connettono a workstation e PC di solito mediante semplici hub o switch. Ciascun nodo (singolo computer) in una LAN dispone della propria CPU con cui esegue programmi, ma è anche in grado di accedere ai dati e ai dispositivi (ad esempio le stampanti) presenti in qualsiasi punto della LAN. In tal modo, molti utenti possono condividere dispositivi costosi, come le stampanti laser, nonché i dati. Gli utenti, inoltre, possono utilizzare la LAN per comunicare tra di loro, ad esempio inviando messaggi di posta elettronica o avviando sessioni di chat.

Larghezza di banda

Quantità di dati trasmettibili in una lasso di tempo fisso. Per i dispositivi digitali, la larghezza di banda di solito viene espressa in bit per secondo (bps) o byte per secondo. Per i dispositivi analogici, la larghezza di banda viene espressa in cicli per secondo o Hertz (Hz).

M

MAC (Media Access Control o Message Authenticator Code)

Per il primo significato, vedere Indirizzo MAC. Il secondo è un codice utilizzato per identificare un determino messaggio (ad esempio, un messaggio RADIUS). Il codice generalmente è un hash dei contenuti del messaggio sottoposto a potente crittografica, che include un valore univoco per garantire una protezione contro la riproduzione.

N

Negazione del servizio

Su Internet un attacco di negazione del servizio (DoS - Denial of Service) è un incidente durante il quale un utente o un'organizzazione vengono privati dei servizi di una risorsa solitamente disponibile. Una tipica perdita di servizio è la mancanza di disponibilità di un particolare servizio di rete, ad esempio la posta elettronica, o la perdita temporanea di tutti i servizi e della connettività di rete. Nei casi peggiori, ad esempio, un sito Web a cui accedono milioni di persone può essere occasionalmente forzato a interrompere temporaneamente il funzionamento. Un attacco di negazione del servizio può anche distruggere i programmi e i file in un sistema informatico. Per quanto di solito sia intenzionale e pericoloso, un attacco di negazione del servizio talvolta può capitare accidentalmente. Un attacco di negazione del servizio è un tipo di violazione della protezione di un sistema informatico che di solito non comporta il furto di informazioni o altre perdite di protezione. Tuttavia, questi attacchi possono costare alla persona o all'azienda che li riceve una gran quantità di tempo e denaro.

NIC (Network Interface Card)

Scheda che si inserisce in un laptop o in altro dispositivo e connette il dispositivo alla LAN.

O

P

PPPoE

Point-to-Point Protocol Over Ethernet (Protocollo punto a punto su Ethernet). Utilizzato da molti provider DSL, PPPoE supporta i livelli di protocollo e l'autenticazione ampiamente utilizzata in PPP e consente di stabilire la connessione point-to-point nell'architettura solitamente multipunto di Ethernet.

Protocollo

Formato concordato per la trasmissione di dati tra due dispositivi. Dal punto di vista di un utente, l'unico aspetto rilevante dei protocolli è che il computer o il dispositivo deve supportare quelli appropriati, se desidera comunicare con altri computer. Il protocollo può essere implementato nell'hardware o nel software.

Q

R

RADIUS (Remote Access Dial-In User Service)

Protocollo che fornisce l'autenticazione degli utenti, di solito nel contesto dell'accesso remoto. Inizialmente definito per l'uso con i server di accesso remoto dial-in, il protocollo viene ora utilizzato in un'ampia gamma di ambienti di autenticazione, inclusa l'autenticazione 802.1x di un segreto condiviso degli utenti di una WLAN.

Rete

Insieme di access point e dei relativi utenti, equivalente a un ESS. Informazioni su questa rete vengono gestite in McAfee Wireless Home Network Security. Vedere ESS.

Roaming

Capacità di spostarsi da un'area a copertura AP a un'altra senza interruzione di servizio o perdita di connettività.

Router

Dispositivo di rete che inoltra pacchetti da una rete all'altra. Sulla base di tabelle di instradamento interne, i router leggono ogni pacchetto in ingresso e decidono come inoltrarlo. L'interfaccia sul router alla quale i pacchetti in uscita vengono inviati può essere determinata da una combinazione dell'indirizzo di origine e di destinazione, nonché dalle attuali condizioni di traffico come carico, costi della linea e linee non valide. Talvolta sono denominati access point (AP).

S

Schede senza fili PCI

Connettono un computer desktop a una rete. La scheda si inserisce in uno slot di espansione PCI all'interno del computer.

Schede senza fili USB

Forniscono un'interfaccia seriale Plug and Play espandibile. Questa interfaccia fornisce una connessione senza fili standard e a basso costo per periferiche come tastiere, mouse, joystick, stampanti, scanner, dispositivi di archiviazione e videocamere per conferenze.

Segreto condiviso

Vedere anche RADIUS. Protegge parti riservate dei messaggi RADIUS. Il segreto condiviso è una password che può essere condivisa dall'autenticatore e dal server di autenticazione in maniera protetta.

Spoofing degli indirizzi IP

Contraffazione di indirizzi IP in un pacchetto IP. Viene utilizzato in molti tipi di attacchi, incluso il dirottamento di sessione. Viene inoltre impiegato per contraffare le intestazioni dei messaggi di posta elettronica di SPAM in modo da impedirne la corretta individuazione.

SSID (Service Set Identifier)

Nome di rete per i dispositivi in un sottosistema LAN senza fili. Si tratta di una stringa di testo non crittografata, contenente 32 caratteri, aggiunta all'inizio di ogni pacchetto WLAN. L'SSID differenzia una WLAN dall'altra, per cui tutti gli utenti di una rete devono fornire lo stesso SSID per accedere a un determinato AP. L'SSID impedisce l'accesso a qualsiasi dispositivo client che non disponga dell'SSID. Tuttavia, per impostazione definita un access point (AP) trasmette il proprio SSID nella sua ricetrasmittente. Anche se la trasmissione SSID è disattivata, un hacker può rilevare l'SSID attraverso lo sniffing.

SSL (Secure Sockets Layer)

Protocollo sviluppato da Netscape per la trasmissione di documenti privati tramite Internet. L'SSL funziona utilizzando una chiave pubblica per crittografare i dati trasferiti sulla connessione SSL. Sia Netscape Navigator che Internet Explorer utilizzano e supportano SSL e molti siti Web utilizzano il protocollo per ottenere informazioni riservate dell'utente, come i numeri di carta di credito. Per convenzione, gli URL che richiedono una connessione SSL iniziano con https: invece di http:.

T

Testo in codice

Dati crittografati. Il testo in codice è illeggibile finché non viene convertito in testo normale (decrittografato) con una chiave.

Testo normale

Qualsiasi messaggio non crittografato.

TKIP (Temporal Key Integrity Protocol)

Metodo di correzione rapida per superare la debolezza inerente alla protezione WEP, in particolare il riutilizzo delle chiavi di crittografia. TKIP modifica le chiavi temporali ogni 10.000 pacchetti, fornendo un metodo di distribuzione dinamica che migliora notevolmente la protezione della rete. Il processo (di protezione) TKIP inizia con una chiave temporale da 128 bit condivisa tra client e access point (AP). TKIP combina la chiave temporale con l'indirizzo MAC (del computer client) e aggiunge un vettore di inizializzazione da 16 ottetti relativamente grande per produrre la chiave che crittografa i dati. Questa procedura assicura che ogni stazione utilizzi flussi di chiavi differenti per crittografare i dati. TKIP utilizza RC4 per eseguire la crittografia. WEP utilizza anche RC4.

U

V

VPN (Virtual Private Network)

Rete costruita utilizzando cavi pubblici per la riunione dei nodi. Ad esempio, esistono molti sistemi che consentono di creare reti utilizzando Internet come mezzo di trasmissione dei dati. Tali sistemi utilizzano la crittografia e altri meccanismi di protezione per garantire che solo gli utenti autorizzati possano accedere alla rete e che i dati non possano essere intercettati.

W

Wardriver

Intrusi armati di laptop, software speciale e qualche hardware di fortuna che girano per città, sobborghi e parchi aziendali per intercettare il traffico LAN senza fili.

WEP (Wired Equivalent Privacy)

Protocollo di crittografia e autenticazione definito come parte dello standard 802.11. Le versioni iniziali sono basate su codici RC4 e sono caratterizzate da una notevole vulnerabilità. WEP tenta di fornire la protezione crittografando i dati su onde radio, in modo che siano protetti durante la trasmissione da un'estremità all'altra. Tuttavia, si è scoperto che WEP non è tanto sicuro come si credeva.

Wi-Fi (Wireless Fidelity)

Utilizzato genericamente quando ci si riferisce a qualunque tipo di rete 802.11, che sia 802.11b, 802.11a, dual-band, ecc. Il termine è utilizzato da Wi-Fi Alliance.

Wi-Fi Alliance

Organizzazione costituita da fornitori leader nel software e nei dispositivi senza fili con la missione di (1) certificare l'interfunzionalità di tutti i prodotti basati su 802.11 e di (2) promuovere il termine Wi-Fi come nome di marchio globale in tutti i mercati per qualsiasi prodotto LAN senza fili basato su 802.11. L'organizzazione funge da consorzio, laboratorio di collaudo e centro di raccolta e smistamento per i fornitori che desiderano promuovere l'interfunzionalità e lo sviluppo di questo settore.

Mentre tutti i prodotti 802.11a/b/g sono detti Wi-Fi, solo i prodotti che hanno superato la verifica Wi-Fi Alliance possono essere definiti Wi-Fi Certified (un marchio registrato). I prodotti che superano la verifica mostrano un sigillo di identificazione sulla confezione che segnala il prodotto come Wi-Fi Certified e che indica la banda di frequenza radio utilizzata. Questo gruppo prima era noto con il nome di Wireless Ethernet Compatibility Alliance (WECA), ma ha modificato il nome nell'ottobre 2002 per rispecchiare meglio il marchio Wi-Fi che desidera costruire.

Wi-Fi Certified

Tutti i prodotti collaudati e approvati come Wi-Fi Certified (un marchio registrato) da Wi-Fi Alliance sono interfunzionanti gli uni con gli altri, anche se realizzati da produttori diversi. Un utente che dispone di un prodotto Wi-Fi Certified può utilizzare un access point (AP) di qualunque marchio con hardware client di qualsiasi altro marchio altrettanto certificato. Tuttavia, in genere, tutti i prodotti Wi-Fi che utilizzano la stessa frequenza di onde radio (ad esempio, 2,4 GHz per 802.11b o 11g, 5 GHz per 802.11a) di altri prodotti funzionano senza problemi, anche se non sono Wi-Fi Certified.

WLAN (Wireless Local Area Network)

Vedere anche LAN. Rete locale che utilizza supporto senza fili per la connessione. Per comunicare tra nodi, una WLAN utilizza onde radio ad alta frequenza anziché cavi.

WPA (Wi-Fi Protected Access)

Standard di specifiche che aumenta notevolmente il livello di protezione dei dati e il controllo dell'accesso dei sistemi LAN senza fili esistenti e futuri. Progettato per funzionare sull'hardware esistente come aggiornamento software, WPA è derivato dallo standard IEEE 802.11i ed è compatibile con esso. Se correttamente installato, garantisce agli utenti della LAN senza fili un elevato livello di protezione dei dati e che solo utenti di rete autorizzati potranno accedere alla rete.

WPA-PSK

Una speciale modalità WPA progettata per gli utenti privati che non richiedono una potente protezione di classe aziendale e non hanno accesso a server di autenticazione. In tal modo, l'utente privato inserisce manualmente la password iniziale per attivare l'accesso protetto Wi-Fi in modalità PSK (Chiave già condivisa) e deve regolarmente cambiare la passphrase su ogni access point e computer senza fili. Vedere anche TKIP.

X

Y

Z

McAfee VirusScan 3

Benvenuti in McAfee VirusScan.

McAfee VirusScan è un servizio antivirus ad abbonamento che offre una protezione antivirus completa, affidabile e aggiornata. Basato sulla notissima tecnologia di scansione di McAfee, VirusScan protegge da virus, worm, cavalli di Troia, script sospetti, attacchi di vario genere e altre minacce.

Grazie a questo software, è possibile usufruire delle seguenti funzioni:

ActiveShield: esegue la scansione dei file quando vengono aperti dall'utente o dal computer.

Scansione: ricerca di virus e altre minacce nei dischi rigidi, nei dischi floppy e nei singoli file e cartelle.

Quarantena: crittografia e isolamento temporaneo nella cartella di quarantena dei file sospetti fino a quando non è possibile effettuare le operazioni appropriate.

Rilevamento di attività ostili: controllo nel computer di attività di tipo virale causate da script sospetti e attività simili a worm.

Nuove funzioni

Questa versione di VirusScan offre le nuove funzioni indicate di seguito:

- **Rilevamento e rimozione di spyware e adware**
  VirusScan identifica e rimuove spyware, adware e altri programmi in grado di compromettere la privacy e rallentare le prestazioni del computer.

- **Aggiornamenti automatici giornalieri**
  Gli aggiornamenti automatici di VirusScan consentono di aggiornare la protezione del computer nei confronti delle più recenti minacce identificate e non identificate.

- **Scansione in background**
  Veloci scansioni identificano e distruggono con discrezione virus, cavalli di Troia, worm, spyware, adware, dialer e altre minacce senza interrompere il lavoro dell'utente.

- **Avvisi di protezione in tempo reale**
  Gli avvisi di protezione notificano all'utente la presenza di epidemie di virus e minacce di protezione e forniscono opzioni di risposta che consentono di rimuovere, neutralizzare o conoscere meglio la minaccia.

- **Rilevamento e pulizia in più punti di accesso**
  VirusScan esegue il monitoraggio e la pulizia nei principali punti di accesso del computer: messaggi di posta elettronica, allegati di messaggi immediati e download di Internet.

- **Monitoraggio della posta elettronica per attività simili a worm**
  WormStopper™ esegue il monitoraggio delle operazioni sospette di mass-mailing e impedisce che virus e worm si diffondano via e-mail in altri computer.

- **Monitoraggio degli script per attività simili a worm**
  ScriptStopper™ esegue il monitoraggio di operazioni sospette di esecuzione di script e impedisce che virus e worm si diffondano via e-mail in altri computer.

- **Supporto tecnico gratuito tramite posta elettronica e messaggistica immediata**
  Il supporto tecnico dal vivo fornisce assistenza in maniera semplice e tempestiva tramite posta elettronica e messaggistica immediata.

Verifica di VirusScan

Prima di utilizzare VirusScan per la prima volta, è consigliabile verificare l'installazione. Attenersi alla seguente procedura per verificare separatamente le funzioni ActiveShield e di scansione.

Verifica di ActiveShield

NOTA
Per verificare ActiveShield dalla scheda VirusScan in SecurityCenter, fare clic su **Prova VirusScan** per visualizzare le domande frequenti online di supporto contenenti questa procedura.

Per verificare ActiveShield:

1. Aprire il browser Web e accedere al sito http://www.eicar.com/.
2. Fare clic sul collegamento **The AntiVirus testfile eicar.com** (File eicar.com di test per antivirus).
3. Scorrere fino in fondo alla pagina. In **Download** sono disponibili quattro collegamenti.
4. Fare clic su **eicar.com**.

Se ActiveShield funziona correttamente, il file eicar.com verrà rilevato immediatamente appena si fa clic sul collegamento. È possibile provare a eliminare o mettere in quarantena i file rilevati per vedere come vengono gestite le possibili minacce. Per ulteriori informazioni, vedere la sezione *Informazioni sugli avvisi di protezione* a pagina 64.

Verifica della funzione Scansione

Prima di poter verificare la funzione Scansione, è necessario disattivare ActiveShield per evitare che rilevi i file di prova prima della funzione di scansione, quindi scaricare i file di prova.

Per scaricare i file di prova:

1 Disattivare ActiveShield: fare clic con il pulsante destro del mouse sull'icona McAfee, scegliere **VirusScan**, quindi fare clic su **Disattiva**.

2 Scaricare i file di prova EICAR dal sito Web della EICAR:

   a Accedere al sito http://www.eicar.com/.

   b Fare clic sul collegamento **The AntiVirus testfile eicar.com** (File eicar.com di test per antivirus).

   c Scorrere fino in fondo alla pagina. In **Download** sono disponibili questi collegamenti:

      eicar.com contiene una riga di testo che viene rilevata come virus da VirusScan.

      eicar.com.txt (opzionale) è lo stesso file, ma con un nome diverso, per gli utenti che hanno difficoltà a scaricare il primo. Rinominare semplicemente il file in "eicar.com" una volta scaricato.

      eicar_com.zip è una copia del virus di prova in un file compresso .ZIP, ossia un archivio di file WinZip™.

      eicarcom2.zip è una copia del virus di prova in un file compresso .ZIP, che a sua volta si trova in un file compresso .ZIP.

   d Fare clic su ogni collegamento per scaricare il rispettivo file. Per ciascun file viene visualizzata la finestra di dialogo **Download file**.

   e Fare clic su **Salva**, selezionare il pulsante **Crea nuova cartella** e rinominare la **Cartella scansione VSO**.

   f Fare doppio clic sulla **Cartella scansione VSO**, quindi selezionare nuovamente **Salva** in ogni finestra di dialogo **Salva con nome**.

3 Al termine del download dei file, chiudere Internet Explorer.

4 Attivare ActiveShield: fare clic con il pulsante destro del mouse sull'icona McAfee, scegliere **VirusScan**, quindi fare clic su **Attiva**.

Per verificare la funzione di scansione:

1 Fare clic con il pulsante destro del mouse sull'icona McAfee, scegliere **VirusScan**, quindi fare clic su **Scansione**.

2 Utilizzando la struttura delle directory nel riquadro di sinistra della finestra di dialogo, andare alla **Cartella scansione VSO** in cui erano stati salvati i file:

   a Fare clic sul segno **+** accanto all'icona dell'unità C.

   b Fare clic su **Cartella scansione VSO** per evidenziare tale cartella. Non fare clic sul segno **+** accanto alla cartella.

   In questo modo la ricerca viene eseguita solo nella cartella specificata. In alternativa, è possibile spostare i file in posizioni casuali nel disco rigido per ottenere una dimostrazione più convincente delle capacità della funzione di scansione.

3 Nell'area **Opzioni di scansione** della finestra di dialogo **Scansione**, verificare che siano selezionate tutte le opzioni.

4 Fare clic su **Scansione** nella parte inferiore della finestra di dialogo.

   Rinominare la **Cartella scansione VSO**. I file di prova EICAR salvati in quella cartella vengono visualizzati nell'**Elenco dei file rilevati**. In tal caso, la scansione funziona correttamente.

È possibile provare a eliminare o mettere in quarantena i file rilevati per vedere come vengono gestite le possibili minacce. Per ulteriori informazioni, vedere la sezione *Informazioni sul rilevamento delle minacce* a pagina 74.

Utilizzo di McAfee VirusScan

Questa sezione descrive come usare VirusScan.

Utilizzo di ActiveShield

Quando viene avviato (caricato nella memoria del computer) e attivato, ActiveShield protegge continuamente il computer. ActiveShield esegue la scansione dei file quando vengono aperti dall'utente o dal computer. Quando ActiveShield rileva un file, cerca automaticamente di pulirlo. Se questa operazione non riesce, è possibile mettere in quarantena o eliminare il file.

Attivazione o disattivazione di ActiveShield

ActiveShield viene avviato (caricato nella memoria del computer) e attivato (indicato dall'icona rossa nella barra delle applicazioni di Windows) per impostazione predefinita appena si riavvia il computer al termine dell'installazione.

Se ActiveShield viene interrotto (non caricato) o è disattivato (indicato dall'icona nera), sarà possibile eseguirlo manualmente o configurarne l'esecuzione automatica all'avvio di Windows.

Attivazione di ActiveShield

Per attivare ActiveShield solo per questa sessione di Windows:

Fare clic con il pulsante destro del mouse sull'icona McAfee, scegliere **VirusScan**, quindi fare clic su **Attiva**. L'icona McAfee si trasforma in una rossa.

Se ActiveShield è ancora configurato per essere avviato all'avvio di Windows, verrà visualizzato un messaggio che indica che si è protetti dalle minacce. In caso contrario, verrà visualizzata una finestra di dialogo che consente di configurare l'avvio di ActiveShield all'avvio di Windows (Figura 3-1 a pagina 54).

Disattivazione di ActiveShield

Per disattivare ActiveShield solo per questa sessione di Windows:

1 Fare clic con il pulsante destro del mouse sull'icona McAfee, scegliere **VirusScan**, quindi fare clic su **Disattiva**.

2 Fare clic su **Sì** per confermare.

   L'icona McAfee diventa di colore nero .

Se ActiveShield è ancora configurato per essere avviato all'avvio di Windows, il computer sarà protetto nuovamente dalle minacce quando verrà riavviato.

Configurazione delle opzioni di ActiveShield

Nella scheda **ActiveShield** della finestra di dialogo **Opzioni di VirusScan** (Figura 3-1), accessibile facendo clic sull'icona McAfee nella barra delle applicazioni di Windows, è possibile modificare le opzioni di avvio e di scansione di ActiveShield.

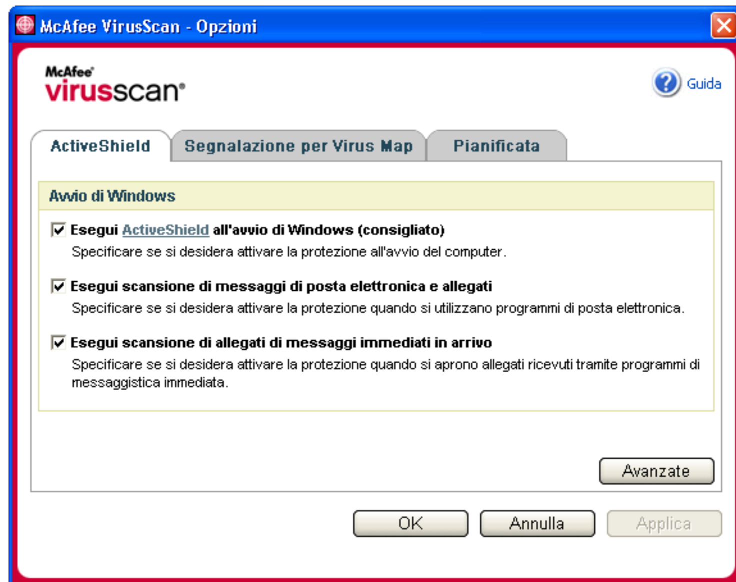


Figura 3-1. Opzioni di ActiveShield

Avvio di ActiveShield

ActiveShield viene avviato (caricato nella memoria del computer) e attivato (indicato dall'icona rossa) per impostazione predefinita appena si riavvia il computer al termine dell'installazione.

Se ActiveShield non è attivato (indicato dall'icona nera), è possibile configurarne l'avvio automatico all'avvio di Windows (consigliato).

NOTA

Durante gli aggiornamenti di VirusScan, ActiveShield potrebbe venire temporaneamente disattivato dalla **procedura guidata di aggiornamento** per consentire l'installazione dei nuovi file. Quando nella **procedura guidata di aggiornamento** viene chiesto di fare clic su **Fine**, ActiveShield viene riavviato.

Per avviare ActiveShield automaticamente all'avvio di Windows:

1. Fare clic con il pulsante destro del mouse sull'icona McAfee, scegliere **VirusScan**, quindi fare clic su **Opzioni**.

   Verrà visualizzata la finestra di dialogo **Opzioni di VirusScan** (Figura 3-1 a pagina 54).

2. Selezionare la casella di controllo **Esegui ActiveShield all'avvio di Windows (consigliato)**, quindi fare clic su **Applica** per salvare le modifiche.

3. Fare clic su **OK** per confermare, quindi nuovamente su **OK**.

Arresto di ActiveShield

ATTENZIONE
Se si arresta ActiveShield, il computer non sarà protetto dalle minacce. Se occorre arrestare ActiveShield, salvo quando si aggiorna VirusScan, accertarsi di non essere connessi a Internet.

Per interrompere l'avvio automatico di ActiveShield all'avvio di Windows:

1. Fare clic con il pulsante destro del mouse sull'icona McAfee, scegliere **VirusScan**, quindi fare clic su **Opzioni**.

   Verrà visualizzata la finestra di dialogo **Opzioni di VirusScan** (Figura 3-1 a pagina 54).

2. Deselezionare la casella di controllo **Esegui ActiveShield all'avvio di Windows (consigliato)**, quindi fare clic su **Applica** per salvare le modifiche.

3. Fare clic su **OK** per confermare, quindi nuovamente su **OK**.

Scansione di messaggi di posta elettronica e allegati

Per impostazione predefinita, l'opzione **Esegui scansione di messaggi di posta elettronica e allegati** (Figura 3-1 a pagina 54) è attivata.

Quando questa opzione è attivata, ActiveShield esegue automaticamente la scansione e tenta di pulire i messaggi di posta elettronica e gli allegati rilevati in ingresso (POP3) e in uscita (SMTP) per i client di posta elettronica più diffusi, tra cui:

- Microsoft Outlook Express 4.0 o versioni successive
- Microsoft Outlook 97 o versioni successive
- Netscape Messenger 4.0 o versioni successive
- Netscape Mail 6.0 o versioni successive

- Eudora Light 3.0 o versioni successive
- Eudora Pro 4.0 o versioni successive
- Eudora 5.0 o versioni successive
- Pegasus 4.0 o versioni successive

NOTA
La scansione della posta elettronica non è supportata per i seguenti client: client basati su Web, IMAP, AOL, POP3 SSL e Lotus Notes. Tuttavia, ActiveShield analizza gli allegati di posta elettronica quando vengono aperti.

Se si disattiva l'opzione **Esegui scansione di messaggi di posta elettronica e allegati**, le opzioni di scansione e le opzioni di WormStopper (Figura 3-2 a pagina 57) vengono disattivate automaticamente. Se si disattiva la scansione dei messaggi di posta elettronica in uscita, le opzioni di WormStopper vengono disattivate automaticamente.

Se si modificano le opzioni di scansione posta, è necessario riavviare il programma di posta elettronica per completare le modifiche.

Messaggi di posta elettronica in ingresso

Se un messaggio di posta elettronica o un allegato in ingresso viene rilevato, ActiveShield esegue le seguenti operazioni:

- Tenta di pulire il messaggio rilevato
- Tenta di mettere in quarantena o eliminare un messaggio che non è possibile pulire
- Include nel messaggio in ingresso un file di avviso che contiene informazioni sulle azioni eseguite per rimuovere l'eventuale minaccia

Messaggi di posta elettronica in uscita

Se un messaggio di posta elettronica o un allegato in uscita viene rilevato, ActiveShield esegue le seguenti operazioni:

- Tenta di pulire il messaggio rilevato
- Tenta di mettere in quarantena o eliminare un messaggio che non è possibile pulire

NOTA
Per informazioni sugli errori di scansione dei messaggi di posta elettronica in uscita, vedere la Guida in linea.

Disattivazione della scansione della posta elettronica

Per impostazione predefinita, ActiveShield esegue la scansione dei messaggi di posta elettronica in ingresso e in uscita. Tuttavia, per un controllo migliore è possibile impostare ActiveShield in modo che effettui solo la scansione dei messaggi di posta elettronica in ingresso o in uscita.

Per disattivare la scansione dei messaggi di posta elettronica in ingresso o in uscita:

1 Fare clic con il pulsante destro del mouse sull'icona McAfee, scegliere **VirusScan**, quindi fare clic su **Opzioni**.

2 Fare clic su **Avanzate**, quindi sulla scheda **Scansione posta** (Figura 3-2).

3 Deselezionare **Messaggi e-mail in ingresso** o **Messaggi e-mail in uscita**, quindi fare clic su **OK**.

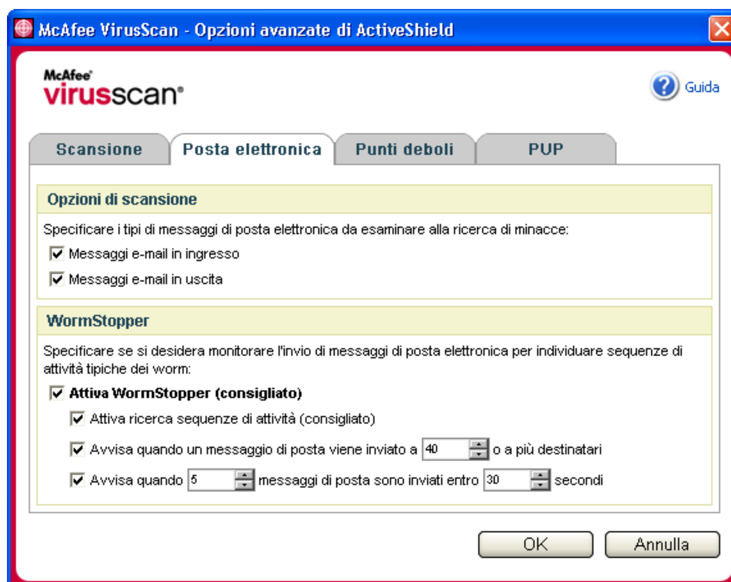


Figura 3-2. Opzioni avanzate di ActiveShield - Scheda Posta elettronica

Ricerca di worm

VirusScan controlla eventuali attività sospette del computer che potrebbero indicare la presenza di una minaccia. VirusScan pulisce i virus ed elimina altre minacce, mentre WormStopper™ impedisce l'ulteriore diffusione di virus e worm.

Un "worm" è un virus in grado di autoreplicarsi; esso risiede nella memoria attiva e può inviare copie di se stesso attraverso la posta elettronica. Senza WormStopper, è possibile notare i worm solo quando l'attività incontrollata di duplicazione consuma le risorse del sistema, rallentando le prestazioni o interrompendo le attività.

Il meccanismo di protezione di WormStopper rileva, avvisa e blocca le attività sospette. Le attività sospette nel computer potrebbero includere:

- Il tentativo di inoltrare un messaggio di posta elettronica a un gran numero di utenti presenti nella propria rubrica
- Tentativi di inoltrare più messaggi di posta elettronica in rapida successione

Se si imposta ActiveShield in modo da utilizzare l'opzione predefinita **Attiva WormStopper (consigliato)** nella finestra di dialogo **Opzioni avanzate**, WormStopper controllerà l'attività della posta elettronica alla ricerca di sequenze sospette e avviserà l'utente se viene superato un numero specifico di messaggi di posta elettronica o destinatari entro un dato intervallo di tempo.

Per impostare ActiveShield in modo che venga eseguita la scansione dei messaggi di posta elettronica inviati, alla ricerca di attività simili a worm:

1. Fare clic con il pulsante destro del mouse sull'icona McAfee, scegliere **VirusScan**, quindi fare clic su **Opzioni**.
2. Fare clic su **Avanzate**, quindi sulla scheda **Posta elettronica**.

3 Fare clic su **Attiva WormStopper (consigliato)** (Figura 3-3).

Per impostazione predefinita, sono attivate le seguenti opzioni dettagliate:

- Ricerca di sequenze di attività per rilevare quelle sospette
- Avviso in caso di invio di messaggi di posta elettronica a 40 o più destinatari
- Avviso in caso di invio di 5 o più messaggi di posta elettronica entro 30 secondi

NOTA
Se si modifica il numero di destinatari o di secondi per il monitoraggio dei messaggi di posta elettronica inviati, è possibile che si verifichino rilevamenti non validi. McAfee consiglia di selezionare **No** per mantenere l'impostazione predefinita. In caso contrario, selezionare **Sì** per personalizzare l'impostazione predefinita.

È possibile attivare automaticamente questa opzione dopo il primo rilevamento di un potenziale worm (per ulteriori informazioni, vedere la sezione *Gestione dei potenziali worm* a pagina 66):

- Blocco automatico di messaggi di posta elettronica sospetti in uscita

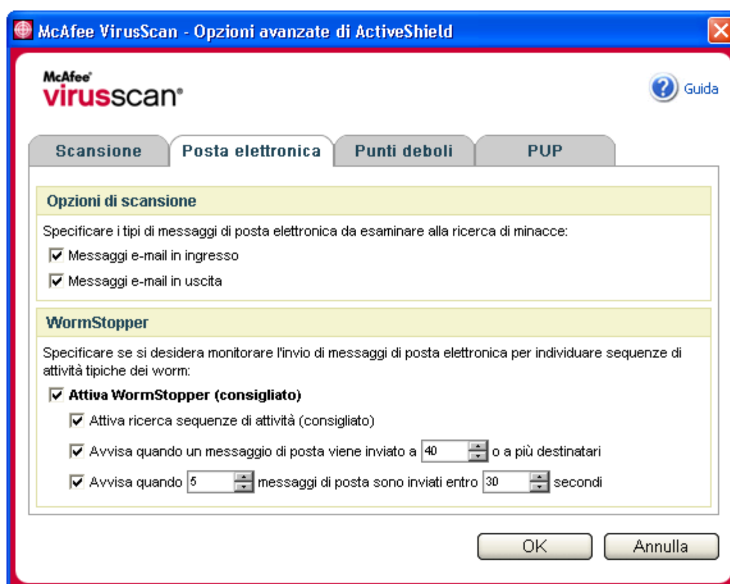


Figura 3-3. Opzioni avanzate di ActiveShield - Scheda Posta elettronica

Scansione degli allegati dei messaggi immediati in ingresso

Per impostazione predefinita, l'opzione **Esegui scansione di allegati di messaggi immediati in arrivo** (Figura 3-1 a pagina 54) è attivata.

Quando questa opzione è attivata, VirusScan esegue automaticamente la scansione e tenta di pulire gli allegati rilevati dei messaggi immediati in ingresso per i programmi di messaggistica immediata più diffusi, tra cui:

- MSN Messenger 6.0 o versioni successive
- Yahoo Messenger 4.1 o versioni successive
- AOL Instant Messenger 2.1 o versioni successive

NOTA
Per una maggiore protezione, non è possibile disattivare la pulizia automatica degli allegati dei messaggi immediati.

Se l'allegato di un messaggio immediato in arrivo viene rilevato, VirusScan esegue le seguenti operazioni:

- Tenta di pulire il messaggio rilevato
- Chiede se mettere in quarantena o eliminare un messaggio che non è possibile pulire

Scansione di tutti i file

Se si imposta ActiveShield in modo da utilizzare l'opzione predefinita **Tutti i file (consigliato)**, verrà eseguita la scansione di tutti i tipi di file utilizzati dal computer appena si tenta di aprirli. Questa opzione offre la scansione più accurata possibile.

Per impostare ActiveShield per eseguire la scansione di tutti i tipi di file:

1. Fare clic con il pulsante destro del mouse sull'icona McAfee, scegliere **VirusScan**, quindi fare clic su **Opzioni**.
2. Fare clic su **Avanzate**, quindi sulla scheda **Scansione** (Figura 3-4 a pagina 61).

3 Fare clic su **Tutti i file (consigliato)**, quindi su **OK**.

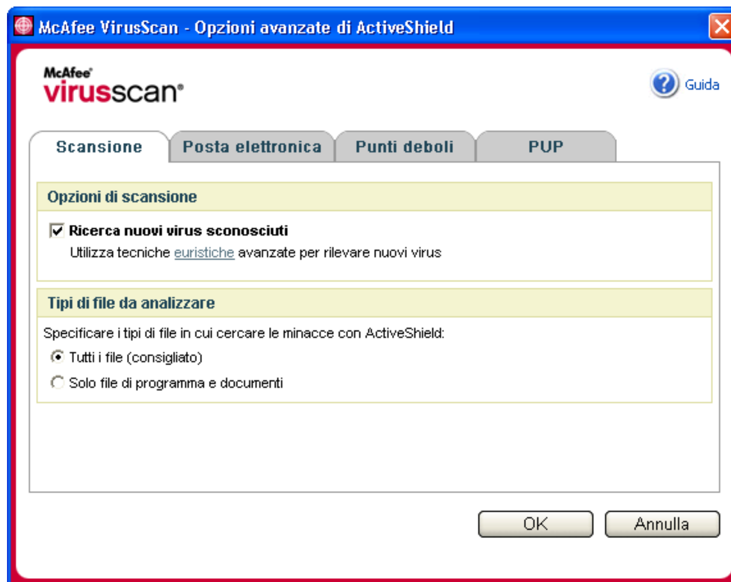


Figura 3-4. Opzioni avanzate di ActiveShield - Scheda Scansione

Scansione esclusivamente di file di programma e documenti

Se si imposta ActiveShield in modo che venga utilizzata l'opzione **Solo file di programma e documenti**, verrà eseguita la scansione dei file di programma e dei documenti, ma non di altri file in uso nel computer. I tipi di file analizzati da ActiveShield vengono determinati dal file più recente delle firme elettroniche dei virus (file DAT). Per impostare ActiveShield per analizzare solo file di programma e documenti:

1 Fare clic con il pulsante destro del mouse sull'icona McAfee, scegliere **VirusScan**, quindi fare clic su **Opzioni**.

2 Fare clic su **Avanzate**, quindi sulla scheda **Scansione** (Figura 3-4).

3 Fare clic su **Solo file di programma e documenti**, quindi su **OK**.

Ricerca di nuovi virus sconosciuti

Se si imposta ActiveShield in modo che utilizzi l'opzione predefinita **Ricerca nuovi virus sconosciuti (consigliato)**, le tecniche euristiche avanzate utilizzate da ActiveShield tentano di far corrispondere i file alle firme elettroniche di virus conosciuti, esaminando nel contempo gli indizi significativi di virus non identificati nei file.

Per impostare ActiveShield per ricercare virus nuovi e sconosciuti:

1 Fare clic con il pulsante destro del mouse sull'icona McAfee, scegliere **VirusScan**, quindi fare clic su **Opzioni**.

2 Fare clic su **Avanzate**, quindi sulla scheda **Scansione** (Figura 3-4).

3 Fare clic su **Ricerca nuovi virus sconosciuti (consigliato)**, quindi su **OK**.

Ricerca di script

VirusScan controlla eventuali attività sospette del computer che potrebbero indicare la presenza di una minaccia. VirusScan pulisce i virus ed elimina altre minacce, mentre ScriptStopper™ impedisce ai cavalli di Troia di eseguire script che diffondono ulteriormente i virus.

Un "cavallo di Troia" è un programma sospetto che finge di essere un'applicazione innocua. I cavalli di Troia non sono virus in quanto non duplicano se stessi, ma possono essere altrettanto distruttivi.

Il meccanismo di protezione di ScriptStopper rileva, avvisa e blocca le attività sospette. Le attività sospette nel computer potrebbero includere:

- L'esecuzione di uno script che causa la creazione, la copia o l'eliminazione di file oppure l'apertura del registro di configurazione di Windows

Se si imposta ActiveShield in modo da utilizzare l'opzione predefinita **Attiva ScriptStopper (consigliato)** nella finestra di dialogo **Opzioni avanzate**, ScriptStopper controllerà l'esecuzione di script alla ricerca di sequenze sospette e avviserà l'utente se viene superato un numero specifico di messaggi di posta elettronica o destinatari entro un dato intervallo di tempo.

Per impostare ActiveShield in modo che venga eseguita la scansione degli script in esecuzione alla ricerca di attività simili a worm:

1 Fare clic con il pulsante destro del mouse sull'icona McAfee, scegliere **VirusScan**, quindi fare clic su **Opzioni**.

2 Fare clic su **Avanzate**, quindi sulla scheda **Punti deboli** (Figura 3-5).

3 Fare clic su **Attiva ScriptStopper (consigliato)** quindi fare clic su **OK**.

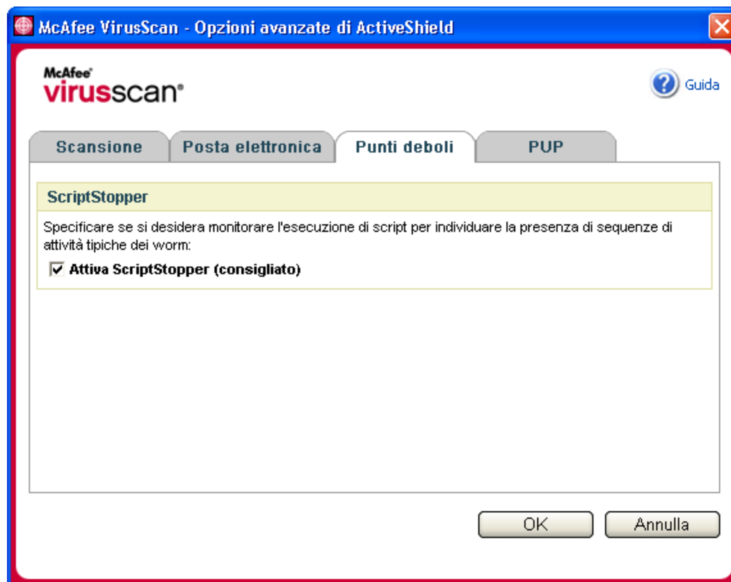


Figura 3-5. Opzioni avanzate di ActiveShield - Scheda Punti deboli

Scansione per la ricerca di programmi potenzialmente indesiderati (PUP)

NOTA
Se è installato nel computer, McAfee AntiSpyware gestisce tutte le attività dei programmi potenzialmente indesiderati. Aprire McAfee AntiSpyware per configurare le opzioni.

Se si imposta ActiveShield in modo da utilizzare l'opzione predefinita **Ricerca programmi potenzialmente indesiderati (consigliato)** nella finestra di dialogo **Opzioni avanzate**, la protezione dai programmi potenzialmente indesiderati (PUP) rileva, blocca e rimuove rapidamente spyware, adware e altri programmi che raccolgono e trasmettono i dati personali senza l'autorizzazione dell'utente.

Per impostare ActiveShield per eseguire la scansione dei PUP:

1 Fare clic con il pulsante destro del mouse sull'icona McAfee, scegliere **VirusScan**, quindi fare clic su **Opzioni**.

2 Fare clic su **Avanzate**, quindi sulla scheda **PUP** (Figura 3-6).

3 Fare clic su **Ricerca programmi potenzialmente indesiderati (consigliato)**, quindi su **OK**.

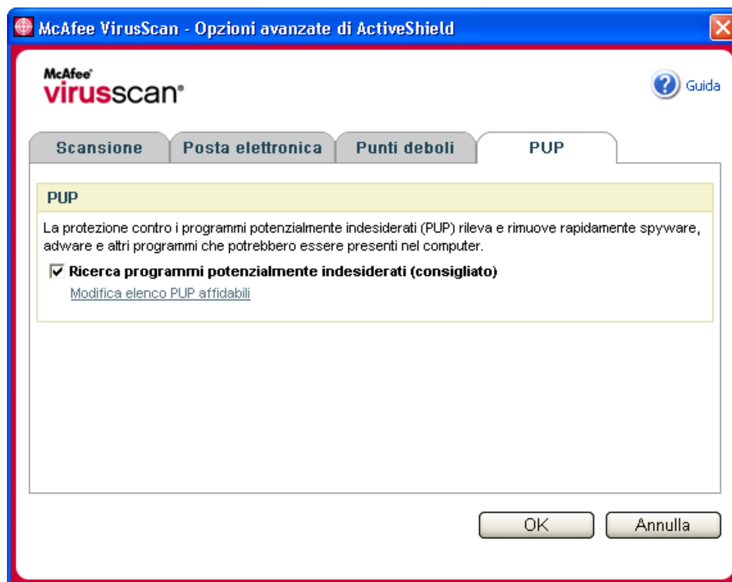


Figura 3-6. Opzioni avanzate di ActiveShield - Scheda PUP

Informazioni sugli avvisi di protezione

Se ActiveShield individua un virus, verrà visualizzato un avviso simile a quello nella Figura 3-7. ActiveShield cerca automaticamente di pulire il file e avvisa l'utente per la maggior parte dei virus, cavalli di Troia e worm. Per i programmi potenzialmente indesiderati (PUP), ActiveShield rileva e blocca automaticamente il file e avvisa l'utente.



Figura 3-7. Avviso di virus

È possibile tuttavia scegliere come gestire i file rilevati, i messaggi di posta elettronica rilevati, gli script sospetti, i potenziali worm o i PUP, nonché decidere se inviare i file rilevati ai laboratori AVERT di McAfee affinché vengano esaminati.

Per maggiore protezione, quando ActiveShield rileva un file sospetto, all'utente viene richiesto di eseguire immediatamente la scansione del computer. Se non si sceglie di nascondere la richiesta di scansione, verrà visualizzato periodicamente un promemoria fino a quando si decide di eseguire la scansione.

Gestione dei file rilevati

1 Se ActiveShield è in grado di pulire il file, è possibile visualizzare ulteriori informazioni o ignorare l'avviso:

   - Fare clic su **Ulteriori informazioni** per visualizzare il nome, il percorso e il nome del virus associati al file rilevato.
   - Fare clic su **Continuare l'operazione in corso** per ignorare e chiudere l'avviso.

2 Se ActiveShield non è in grado di pulire il file, fare clic su **Mettere in quarantena il file infetto** per crittografare e isolare temporaneamente nella directory di quarantena i file sospetti, fino a quando non sarà possibile effettuare le operazioni appropriate.

   Verrà visualizzato un messaggio di conferma e verrà chiesto di cercare le minacce nel computer. Fare clic su **Scansione** per completare il processo di quarantena.

3 Se ActiveShield non è in grado di mettere in quarantena il file, fare clic su **Eliminare il file rilevato** per cercare di rimuoverlo.

Gestione dei messaggi di posta elettronica rilevati

Per impostazione predefinita, la scansione dei messaggi di posta elettronica tenta automaticamente di pulire i messaggi di posta elettronica rilevati. Un file di avviso incluso nel messaggio in entrata notifica all'utente se il messaggio di posta elettronica è stato pulito, messo in quarantena o eliminato.

Gestione degli script sospetti

Se ActiveShield rileva uno script sospetto, è possibile visualizzare ulteriori informazioni, quindi arrestare lo script se non si intendeva avviarlo:

- Fare clic su **Ulteriori informazioni** per visualizzare il nome, il percorso e la descrizione dell'attività associati allo script sospetto.
- Fare clic su **Interrompi script** per evitare l'esecuzione dello script sospetto.

Se si è certi dell'affidabilità dello script, è possibile consentirne l'esecuzione:

- Fare clic su **Consentire esecuzione script** per consentire a tutti gli script contenuti in un singolo file di essere eseguiti una volta.
- Fare clic su **Continuare l'operazione in corso** per ignorare l'avviso e consentire l'esecuzione dello script.

Gestione dei potenziali worm

Se ActiveShield rileva un potenziale worm, è possibile visualizzare ulteriori informazioni, quindi arrestare l'attività di posta elettronica se non si intendeva avviarla:

- Fare clic su **Ulteriori informazioni** per visualizzare l'elenco dei destinatari, la riga dell'oggetto, il corpo del messaggio e la descrizione dell'attività sospetta associata al messaggio di e-mail rilevato.
- Fare clic su **Interrompere questo messaggio di posta elettronica** per evitare l'invio del messaggio sospetto e per eliminarlo dalla coda dei messaggi.

Se si è certi dell'affidabilità dell'attività di posta elettronica, fare clic su **Continuare l'operazione in corso** per ignorare l'avviso e consentire l'avvio del messaggio.

Gestione dei PUP

Se ActiveShield rileva e blocca un programma potenzialmente indesiderato (PUP), è possibile visualizzare ulteriori informazioni, quindi rimuovere il programma se non si intendeva installarlo:

- Fare clic su **Ulteriori informazioni** per visualizzare il nome, il percorso e l'azione consigliata associati al PUP.
- Fare clic su **Rimuovi questo PUP** per rimuovere il programma se non si intendeva installarlo.

  Verrà visualizzato un messaggio di conferma.

  - Se l'utente (a) non riconosce il PUP o (b) non ha installato il PUP come parte di un pacchetto software o non ha accettato un contratto di licenza relativo a tali programmi, fare clic su **OK** per rimuovere il programma utilizzando il metodo di rimozione di McAfee.

  - In caso contrario, fare clic su **Annulla** per chiudere il processo di rimozione automatico. Se in seguito si cambia idea, è possibile rimuovere manualmente il programma utilizzando il relativo programma di disinstallazione.
- Fare clic su **Continuare l'operazione in corso** per ignorare l'avviso e bloccare il programma questa volta.

Se l'utente (a) riconosce il PUP o (b) ha installato il PUP come parte di un pacchetto software o ha accettato un contratto di licenza relativo a tali programmi, è possibile consentirne l'esecuzione:

- Fare clic su **Accetta come affidabile questo PUP** per autorizzare il programma e consentirne l'esecuzione in futuro.

  Per ulteriori informazioni, vedere la sezione *Gestione dei PUP affidabili*.

Gestione dei PUP affidabili

I programmi aggiunti all'elenco **PUP affidabili** non verranno rilevati da McAfee VirusScan.

Se un PUP viene rilevato e aggiunto all'elenco **PUP affidabili**, è possibile rimuoverlo in seguito dall'elenco, se necessario.

Se l'elenco **PUP affidabili** è completo, rimuovere alcune voci prima di potere considerare come affidabile un altro PUP.

Per rimuovere un programma dall'elenco **PUP affidabili**:

1. Fare clic con il pulsante destro del mouse sull'icona McAfee, scegliere **VirusScan**, quindi fare clic su **Opzioni**.
2. Fare clic su **Avanzate**, quindi sulla scheda **PUP**.
3. Fare clic su **Modifica elenco PUP affidabili**, selezionare la casella di controllo in corrispondenza del nome del file e fare clic su **Rimuovi.** Al termine della rimozione delle voci, fare clic su **OK**.

Scansione manuale del computer

La funzione di scansione consente di cercare in modo selettivo virus e altre minacce nei dischi rigidi, nei dischi floppy e nei singoli file e cartelle. Quando viene individuato un file sospetto, la funzione di scansione tenta automaticamente di pulire il file, a meno che non si tratti di un programma potenzialmente indesiderato. Se questa operazione non riesce, il file verrà messo in quarantena o eliminato.

Ricerca manuale di virus e altre minacce

Per eseguire la scansione del computer:

1 Fare clic con il pulsante destro del mouse sull'icona McAfee, scegliere **VirusScan**, quindi fare clic su **Scansione**.

Viene visualizzata la finestra di dialogo **Scansione** (Figura 3-8).

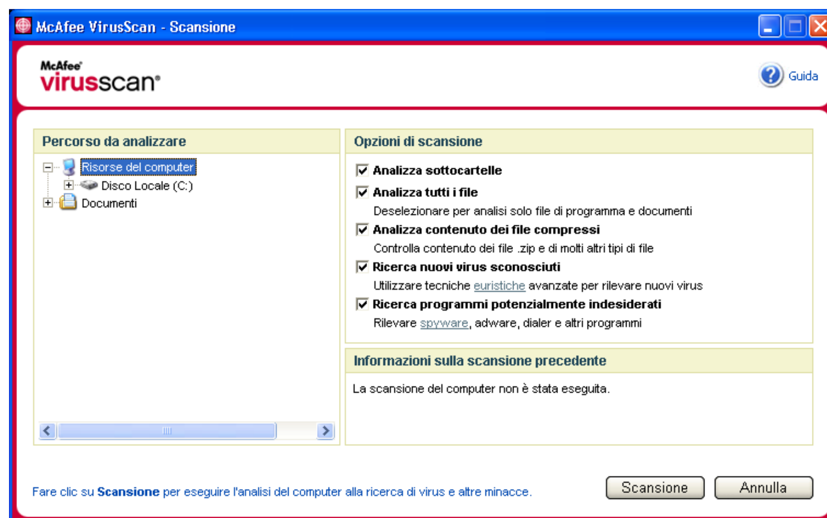


Figura 3-8. Finestra di dialogo Scansione

2 Fare clic sull'unità, sulla cartella o sul file di cui si desidera effettuare la scansione.

3 Selezionare le **Opzioni di scansione**. Per impostazione predefinita, tutte le **Opzioni di scansione** sono preselezionate per offrire la scansione più accurata possibile (Figura 3-8):

- **Analizza sottocartelle**: questa opzione consente di eseguire la scansione dei file contenuti nelle sottocartelle. Deselezionare questa casella di controllo per consentire il controllo dei soli file visibili quando si apre una cartella o un'unità.

  Esempio: i file nella Figura 3-9 sono i soli file analizzati se si deseleziona la casella di controllo **Analizza sottocartelle**. In questo caso le cartelle e il relativo contenuto non vengono analizzati. Per eseguirne la scansione è necessario lasciare selezionata la casella di controllo.

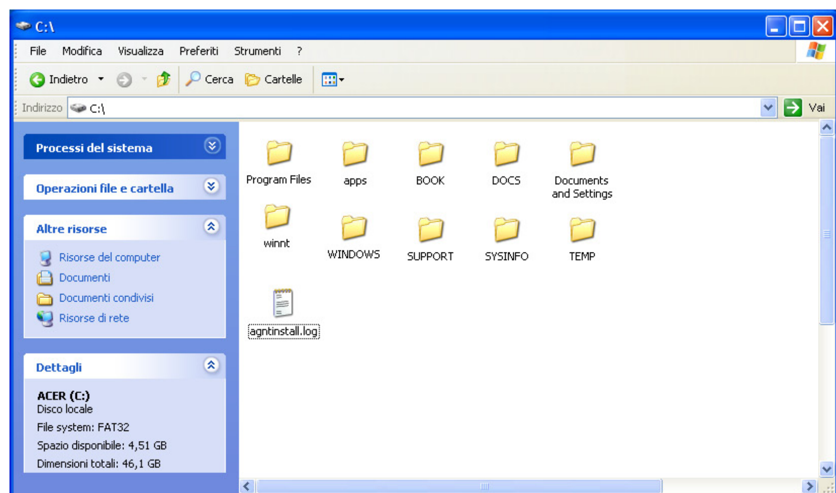


Figura 3-9. Contenuto del disco locale

- **Analizza tutti i file**: questa opzione consente di eseguire una scansione accurata di tutti i tipi di file. Deselezionare questa casella di controllo per ridurre i tempi di scansione e consentire solo la scansione dei file di programma e dei documenti.

- **Analizza contenuto dei file compressi**: questa opzione consente di rilevare i file nascosti nei file .ZIP e in altri file compressi. Deselezionare questa casella di controllo per evitare l'analisi dei file compressi o dei file contenuti nei file compressi.

  Talvolta gli autori dei virus inseriscono i virus in un file .ZIP, quindi inseriscono questo file .ZIP in un altro file .ZIP per tentare di superare le barriere dei programmi antivirus. La selezione della presente opzione consente di rilevare anche questi virus.

- **Ricerca nuovi virus sconosciuti**: questa opzione consente di trovare i virus più recenti, per i quali potrebbe non essere ancora disponibile un rimedio. Questa opzione utilizza tecniche euristiche avanzate che tentano di far corrispondere i file alle firme elettroniche di virus conosciuti, esaminando al contempo gli indizi significativi di virus non identificati nei file.

  Questo metodo di scansione esamina anche le caratteristiche dei file che in genere indicano la presenza di un virus. In questo modo, le possibilità di un'indicazione errata sono ridotte al minimo. In ogni caso, se viene rilevato un virus con una scansione euristica, è consigliabile trattare il file con le stesse precauzioni che si applicherebbero per un file che contiene sicuramente un virus.

  Questa opzione fornisce la scansione più accurata, ma in genere è più lenta di una scansione normale.

- **Ricerca programmi potenzialmente indesiderati** : utilizzare questa opzione per rilevare spyware, adware e altri programmi che raccolgono e trasmettono informazioni personali senza autorizzazione.

  NOTA
  Lasciare tutte le opzioni selezionate per effettuare la scansione più accurata possibile. In questo modo vengono analizzati tutti i file presenti nell'unità o nella cartella selezionate, quindi la scansione potrebbe richiedere molto tempo. Maggiori sono la dimensione del disco rigido e il numero di file, maggiore sarà la durata della scansione.

4 Per avviare la scansione dei file, fare clic su **Scansione**.

Al termine della scansione, un riepilogo della scansione mostra il numero di file analizzati, il numero di file rilevati, il numero di programmi potenzialmente indesiderati e il numero di file rilevati che sono stati puliti automaticamente.

5 Fare clic su **OK** per chiudere il riepilogo e visualizzare l'elenco dei file rilevati nella finestra di dialogo **Scansione** (Figura 3-10).

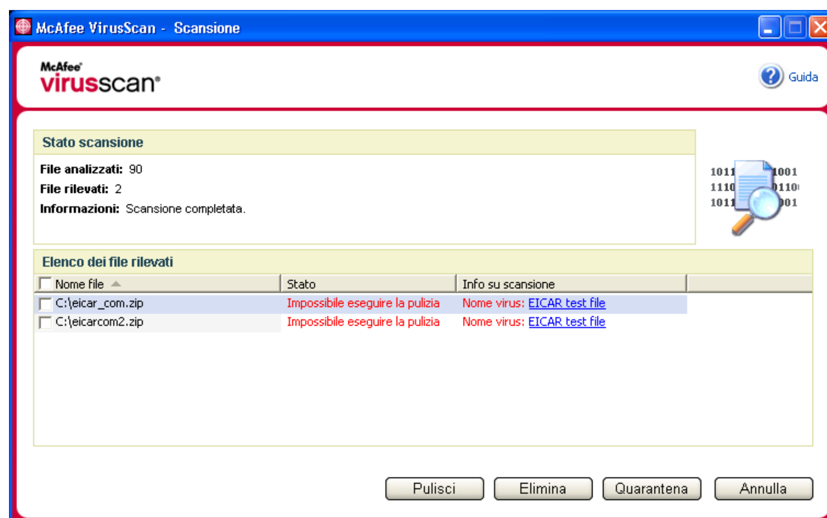


Figura 3-10. Risultati della scansione

NOTA
La scansione conta un file compresso (.ZIP, .CAB e così via) come un file nel numero di **File analizzati**. Inoltre, il numero di file analizzati può variare se si sono eliminati i file temporanei di Internet dopo l'ultima scansione.

6 Se non vengono individuati virus o altre minacce, fare clic su **Indietro** per selezionare un'altra unità o un'altra cartella da analizzare oppure fare clic su **Chiudi** per chiudere la finestra di dialogo. In caso contrario, vedere *Informazioni sul rilevamento delle minacce* a pagina 74.

Scansione tramite Esplora risorse

VirusScan fornisce un menu di scelta rapida per cercare virus e altre minacce nei file, nelle cartelle o nelle unità selezionate in Esplora risorse.

Per analizzare i file in Esplora risorse:

1 Aprire Esplora risorse.

2 Fare clic con il pulsante destro del mouse sull'unità, la cartella o il file da analizzare, quindi scegliere **Scansione**.

Viene aperta la finestra di dialogo **Scansione** e ha inizio la scansione dei file. Per impostazione predefinita, tutte le **Opzioni di scansione** predefinite sono preselezionate per offrire la scansione più accurata possibile (Figura 3-8 a pagina 68).

Scansione tramite Microsoft Outlook

VirusScan include un'icona della barra degli strumenti per rilevare virus e altre minacce in archivi di messaggi selezionati e rispettive sottocartelle, cartelle delle caselle della posta oppure messaggi di posta elettronica che contengono allegati in Microsoft Outlook 97 o versioni successive.

Per eseguire la scansione della posta elettronica in Microsoft Outlook:

1 Aprire Microsoft Outlook.

2 Fare clic sull'archivio di messaggi, sulla cartella o sul messaggio di posta elettronica che contiene un allegato da analizzare, quindi fare clic sull'icona di scansione della posta nella barra degli strumenti .

Lo scanner della posta viene aperto e inizia la scansione dei file. Per impostazione predefinita, tutte le **Opzioni di scansione** predefinite sono preselezionate per offrire la scansione più accurata possibile (Figura 3-8 a pagina 68).

Ricerca automatica di virus e altre minacce

Sebbene VirusScan analizzi i file non appena vengono aperti dall'utente o dal computer, è possibile pianificare una scansione automatica nell'Utilità di pianificazione di Windows per cercare accuratamente i virus e altre minacce a intervalli di tempo specificati.

Per pianificare una scansione:

1 Fare clic con il pulsante destro del mouse sull'icona McAfee, scegliere **VirusScan**, quindi fare clic su **Opzioni**.

Verrà visualizzata la finestra di dialogo **Opzioni di VirusScan**.

2 Fare clic sulla scheda **Pianificata** (Figura 3-11 a pagina 73).

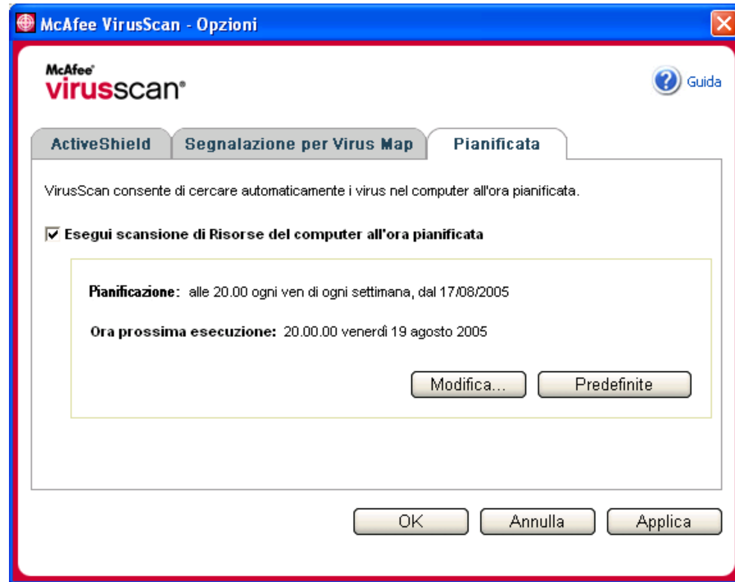


Figura 3-11. Opzioni di scansione pianificata

3 Per attivare la scansione automatica, selezionare la casella di controllo **Esegui scansione di Risorse del computer all'ora pianificata**.

4 Specificare una pianificazione di scansione automatica:

- Per accettare la pianificazione predefinita (alle 20.00 del venerdì di ogni settimana), fare clic su **OK**.
- Per modificare la pianificazione:

  a. Fare clic su **Modifica**.

  b. Selezionare la frequenza di scansione del computer nell'elenco **Pianifica operazione**, quindi selezionare altre opzioni nell'area dinamica sottostante:

  Giornaliera: consente di specificare il numero di giorni tra le scansioni.

  Settimanale (predefinita): consente di specificare il numero di settimane tra le scansioni, nonché i nomi dei giorni della settimana.

  Mensile: consente di specificare il giorno del mese in cui eseguire la scansione. Fare clic su **Seleziona mesi** per specificare i mesi in cui eseguire la scansione, quindi fare clic su **OK**.

Una volta sola: consente di specificare la data in cui eseguire la scansione.

> **NOTA**
> Le seguenti opzioni dell'Utilità di pianificazione di Windows non sono supportate:
> **All'avvio del sistema**, **Quando il PC è inattivo** e **Mostra pianificazioni multiple**. Verrà utilizzata l'ultima pianificazione supportata finché non verrà selezionata un'opzione valida.

c. Nella casella **Ora di inizio**, selezionare l'ora del giorno in cui eseguire la scansione.

d. Per selezionare le opzioni avanzate, fare clic su **Avanzate**.

Verrà visualizzata la finestra di dialogo **Opzioni di pianificazione avanzate**.

i. Specificare una data di inizio, una data di fine, la durata, l'ora di fine e se arrestare l'operazione all'ora specificata se la scansione è ancora in esecuzione.

ii. Fare clic su **OK** per salvare le modifiche apportate e chiudere la finestra di dialogo. In alternativa, fare clic su **Annulla**.

5 Fare clic su **OK** per salvare le modifiche apportate e chiudere la finestra di dialogo. In alternativa, fare clic su **Annulla**.

6 Per tornare alla pianificazione predefinita, fare clic su **Imposta predefinito**. In caso contrario, fare clic su **OK**.

Informazioni sul rilevamento delle minacce

La funzione di scansione cerca automaticamente di pulire il file per la maggior parte dei virus, cavalli di Troia e worm. È possibile tuttavia scegliere come gestire i file rilevati, nonché decidere se inviarli ai laboratori AVERT di McAfee affinché vengano esaminati. Se la funzione di scansione rileva un programma potenzialmente indesiderato, è possibile provare manualmente a pulirlo, metterlo in quarantena o eliminarlo (l'invio ad AVERT non è disponibile).

Per gestire un virus o un programma potenzialmente indesiderato:

1 Se viene visualizzato un file nell'**Elenco dei file rilevati**, fare clic sulla rispettiva casella di controllo per selezionarlo.

> **NOTA**
> Se vengono visualizzati più file nell'elenco, è possibile selezionare la casella di controllo davanti all'elenco **Nome file** per eseguire la stessa operazione su tutti i file. Inoltre, è possibile fare clic sul nome del file nell'elenco **Informazioni sulla scansione** per visualizzare i dettagli provenienti dalla Libreria di informazioni sui virus.

2 Se il file è un programma potenzialmente indesiderato, è possibile selezionare **Pulisci** per tentare la pulizia del file.

3 Se la funzione di scansione non è in grado di pulire il file, fare clic su **Quarantena** per crittografare e isolare temporaneamente nella directory di quarantena i file sospetti, fino a quando non sarà possibile effettuare le operazioni appropriate. Per ulteriori informazioni, vedere la sezione *Gestione dei file in quarantena* a pagina 75.

4 Se la funzione di scansione non è in grado di pulire o mettere in quarantena il file, è possibile effettuare una delle seguenti operazioni:

- Fare clic su **Elimina** per rimuovere il file.
- Fare clic su **Annulla** per chiudere la finestra di dialogo senza effettuare altre operazioni.

Se non è possibile pulire o eliminare il file rilevato, consultare la Libreria di informazioni sui virus all'indirizzo http://it.mcafee.com/virusInfo/ per reperire le istruzioni sull'eliminazione manuale dei virus.

Se il file rilevato impedisce l'uso della connessione a Internet o del computer, provare a utilizzare un disco di ripristino per riavviare il sistema. In molti casi è possibile avviare con un disco di ripristino un computer disattivato da un file rilevato. Per ulteriori informazioni, vedere la sezione *Creazione di un disco di ripristino* a pagina 77.

Per ulteriore assistenza, rivolgersi al Servizio clienti McAfee all'indirizzo http://www.mcafeeaiuto.com.

Gestione dei file in quarantena

La funzione Quarantena consente di crittografare e isolare temporaneamente nella directory di quarantena i file sospetti, fino a quando non sarà possibile effettuare le operazioni appropriate. Dopo la pulizia, i file in quarantena possono essere ripristinati nei percorsi originali.

Per gestire i file in quarantena:

1 Fare clic con il pulsante destro del mouse sull'icona McAfee, scegliere **VirusScan**, quindi fare clic su **Gestione dei file in quarantena**.

Verrà visualizzato un elenco di file in quarantena (Figura 3-12).

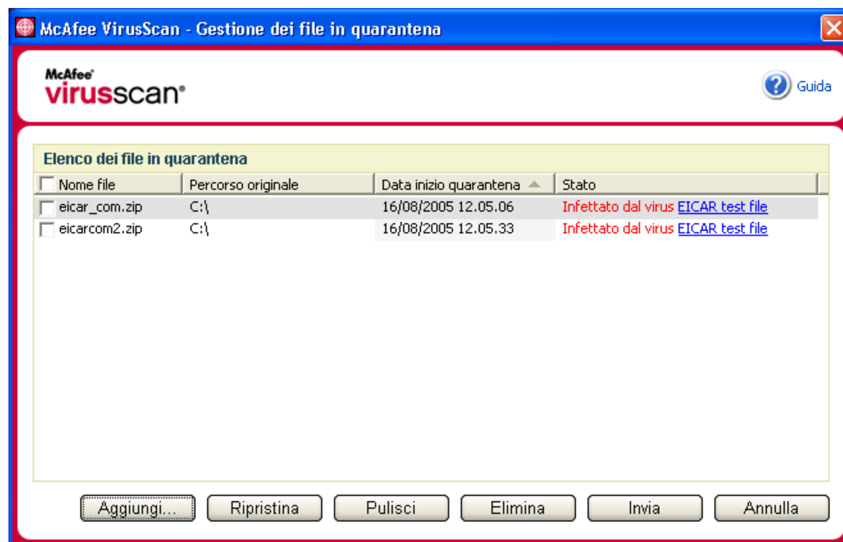


Figura 3-12. Finestra di dialogo Gestione dei file in quarantena

2 Selezionare la casella di controllo accanto al file o ai file da pulire.

NOTA
Se vengono visualizzati più file nell'elenco, è possibile selezionare la casella di controllo davanti all'elenco **Nome file** per eseguire la stessa operazione su tutti i file. Inoltre, è possibile fare clic sul nome del virus nell'elenco **Stato** per visualizzare i dettagli provenienti dalla Libreria di informazioni sui virus.

Oppure, fare clic su **Aggiungi**, selezionare un file sospetto da aggiungere all'elenco in quarantena, fare clic su **Apri**, quindi selezionarlo nell'elenco.

3 Fare clic su **Pulisci**.

4 Se il file viene pulito, fare clic su **Ripristina** per riportarlo nel percorso originale.

5 Se VirusScan non è in grado di pulire il virus, fare clic su **Elimina** per rimuovere il file.

6 Se VirusScan non è in grado di pulire o eliminare il file e se non si tratta di un programma potenzialmente indesiderato, è possibile inviarlo all'AntiVirus Emergency Response Team (AVERT™) di McAfee affinché venga esaminato:

a Aggiornare i file delle firme elettroniche dei virus se risalgono a oltre due settimane prima.

b Verificare l'abbonamento.

c Selezionare il file, quindi fare clic su **Invia** per inviare il file ad AVERT.

VirusScan invia i file in quarantena come allegati in un messaggio di posta elettronica che contiene l'indirizzo di posta elettronica dell'utente, il paese, la versione del software, il sistema operativo e il nome e il percorso originali del file. La dimensione massima di invio è un unico file da 1,5 MB al giorno.

7 Fare clic su **Annulla** per chiudere la finestra di dialogo senza effettuare altre operazioni.

Creazione di un disco di ripristino

Il disco di ripristino è un'utilità che crea un disco floppy avviabile che è possibile utilizzare per avviare il computer ed effettuare la scansione alla ricerca di virus se l'avvio normale è impedito da un virus.

NOTA
Per scaricare l'immagine del disco di ripristino, è necessario essere connessi a Internet. Il disco di ripristino è disponibile solo per i computer con partizioni FAT (FAT 16 e FAT 32) del disco rigido. Non è necessario per le partizioni NTFS.

Per creare un disco di ripristino:

1 In un computer non infetto, inserire un disco floppy non infetto nell'unità A. Si consiglia di utilizzare la funzione di scansione per assicurarsi che non siano presenti virus nel computer e nel disco floppy. Per ulteriori informazioni, vedere la sezione *Ricerca manuale di virus e altre minacce* a pagina 68.

2 Fare clic con il pulsante destro del mouse sull'icona McAfee, scegliere **VirusScan**, quindi fare clic su **Crea disco di ripristino**.

Verrà visualizzata la finestra di dialogo **Crea disco di ripristino** (Figura 3-13).

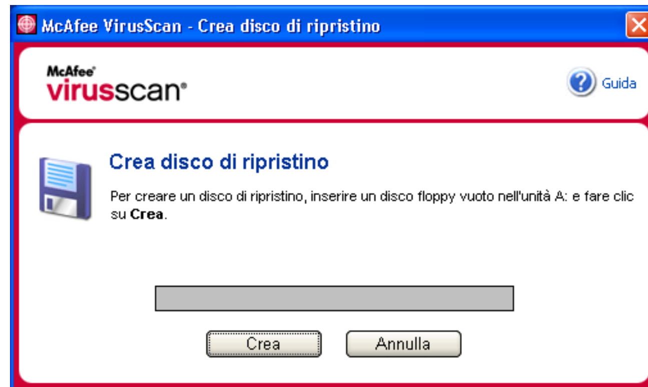


Figura 3-13. Finestra di dialogo Crea disco di ripristino

3 Fare clic su **Crea** per creare il disco di ripristino.

La prima volta che si crea un disco di ripristino viene visualizzato un messaggio in cui si specifica che è necessario scaricare il file immagine per il disco di ripristino. Fare clic su **OK** per scaricare subito il componente oppure su **Annulla** per scaricarlo in un secondo momento.

Viene visualizzato un messaggio di avviso per informare che il contenuto del disco floppy andrà perso.

4 Fare clic su **Sì** per continuare la creazione del disco di ripristino.

Nella finestra di dialogo **Crea disco di ripristino** viene visualizzato lo stato della creazione.

5 Quando viene visualizzato il messaggio "Creazione del disco di ripristino completata", scegliere **OK**, quindi chiudere la finestra di dialogo **Crea disco di ripristino**.

6 Rimuovere il disco di ripristino dall'unità, proteggerlo dalla scrittura e riporlo in un luogo sicuro.

Protezione da scrittura di un disco di ripristino

Per proteggere da scrittura un disco di ripristino:

1 Rivolgere verso il basso il lato con l'etichetta del disco floppy (deve essere visibile il cerchio di metallo).

2 Individuare la linguetta di protezione dalla scrittura. Far scorrere la linguetta in modo che sia visibile il foro.

Utilizzo di un disco di ripristino

Per utilizzare un disco di ripristino:

1 Spegnere il computer infetto.

2 Inserire il disco di ripristino nell'unità.

3 Accendere il computer.

   Verrà visualizzata una finestra grigia con varie opzioni.

4 Scegliere l'opzione che si adatta meglio alle proprie esigenze premendo i rispettivi tasti funzione (ad esempio F2 e F3).

   NOTA
   Se non si preme nessuno di questi tasti entro 60 secondi, verrà avviata automaticamente l'utilità del disco di ripristino.

Aggiornamento di un disco di ripristino

È consigliabile aggiornare regolarmente il disco di ripristino. Per aggiornare il disco di ripristino, attenersi alle istruzioni indicate per la creazione di un disco di ripristino.

Segnalazione automatica dei virus

È possibile inviare in modo anonimo informazioni sui virus da includere nella World Virus Map. È possibile effettuare automaticamente la registrazione per questa funzione gratuita e protetta durante l'installazione di VirusScan (nella finestra di dialogo **Segnalazione per Virus Map**) o in qualsiasi momento nella scheda **Segnalazione per Virus Map** della finestra di dialogo **Opzioni di VirusScan**.

Segnalazione per la World Virus Map

Per segnalare automaticamente le informazioni sui virus alla World Virus Map:

1 Fare clic con il pulsante destro del mouse sull'icona McAfee, scegliere **VirusScan**, quindi fare clic su **Opzioni**.

   Verrà visualizzata la finestra di dialogo **Opzioni di VirusScan**.

2 Fare clic sulla scheda **Segnalazione per Virus Map** (Figura 3-14).

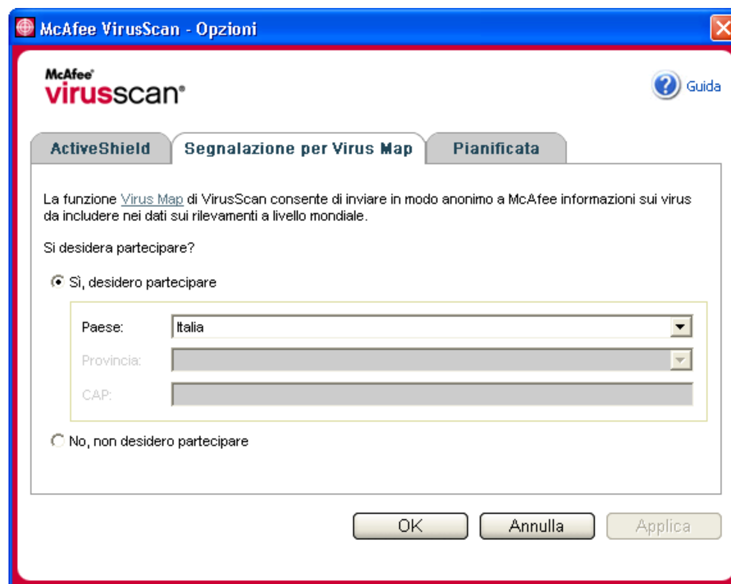


Figura 3-14. Opzioni di Segnalazione per Virus Map

3 Accettare l'opzione predefinita **Sì, desidero partecipare** per inviare in modo anonimo informazioni a McAfee da includere nella World Virus Map delle informazioni sui rilevamenti a livello mondiale. In alternativa, selezionare **No, non desidero partecipare** per non inviare le informazioni.

4 Chi risiede negli Stati Uniti, deve selezionare lo stato e immettere il codice postale dell'area in cui si trova il computer. Chi risiede fuori dagli Stati Uniti, deve selezionare il paese in cui si trova il computer.

5 Fare clic su **OK**.

Visualizzazione della World Virus Map

Indipendentemente dalla partecipazione al programma di segnalazione alla World Virus Map, è possibile visualizzare le informazioni più recenti sui rilevamenti a livello mondiale facendo clic sull'icona McAfee nella barra delle applicazioni di Windows.

Per visualizzare la World Virus Map:

- Fare clic con il pulsante destro del mouse sull'icona McAfee, scegliere **VirusScan**, quindi fare clic su **World Virus Map**.

  Verrà visualizzata la pagina Web **World Virus Map** (Figura 3-15).

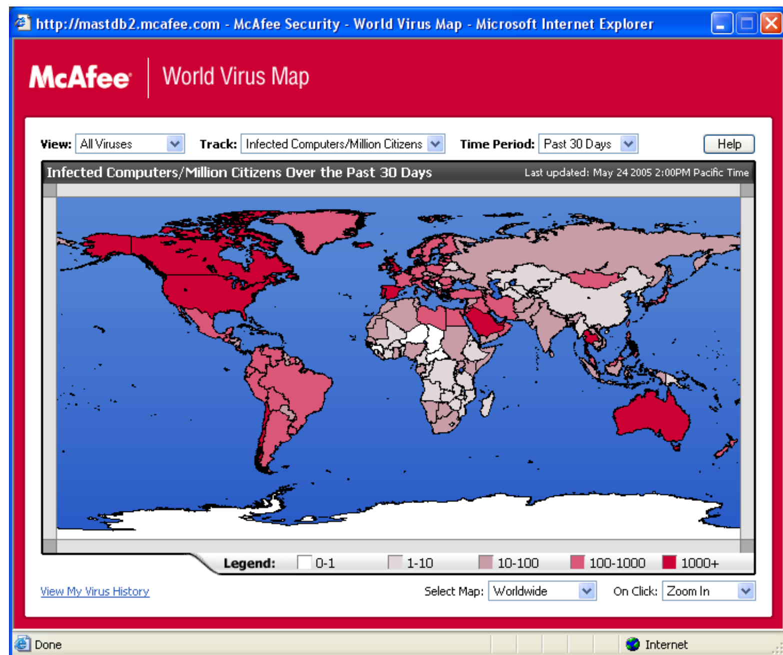


Figura 3-15. World Virus Map

Per impostazione predefinita, la World Virus Map mostra il numero di computer rilevati in tutto il mondo negli ultimi 30 giorni e la data di aggiornamento dei dati. È possibile modificare la visualizzazione in modo da mostrare il numero di file rilevati oppure è possibile modificare il periodo di tempo per visualizzare solo i risultati degli ultimi 7 giorni o delle ultime 24 ore.

Nella sezione Rintracciamento virus sono elencati i totali cumulativi dei file analizzati, dei file rilevati e dei computer rilevati segnalati a partire dalla data indicata.

Aggiornamento di VirusScan

Quando si è connessi a Internet, VirusScan verifica automaticamente la disponibilità di aggiornamenti ogni quattro ore, quindi scarica e installa automaticamente gli aggiornamenti settimanali delle firme elettroniche dei virus (file .dat) senza interrompere le operazioni in corso.

I file .dat hanno una dimensione di circa 100 KB, quindi hanno un impatto minimo sulle prestazioni del sistema durante il download.

In caso di disponibilità di un aggiornamento di un prodotto o di epidemia di virus, verrà visualizzato un avviso. Una volta avvisati, sarà possibile scegliere di aggiornare VirusScan per eliminare la minaccia di un'epidemia di virus.

Verifica automatica della disponibilità di aggiornamenti

McAfee SecurityCenter è configurato automaticamente per verificare gli aggiornamenti di tutti i servizi McAfee ogni quattro ore quando si è connessi a Internet e per notificare tali aggiornamenti con avvisi e segnali acustici. Per impostazione predefinita, SecurityCenter scarica e installa automaticamente tutti gli aggiornamenti disponibili.

NOTA
In alcuni casi, verrà richiesto di riavviare il computer per completare l'aggiornamento. Prima di riavviare, assicurarsi di salvare tutti i dati e chiudere tutte le applicazioni.

Verifica manuale della disponibilità di aggiornamenti

Oltre alla verifica automatica ogni quattro ore durante la connessione a Internet, è possibile verificare manualmente la disponibilità di aggiornamenti in qualsiasi momento.

Per verificare manualmente la disponibilità di aggiornamenti di VirusScan:

1. Assicurarsi che il computer sia connesso a Internet.
2. Fare clic con il pulsante destro del mouse sull'icona McAfee, quindi scegliere **Aggiornamenti**.

   Verrà visualizzata la finestra di dialogo **Aggiornamenti di SecurityCenter**.

3 Fare clic su **Controlla**.

Se è disponibile un aggiornamento, verrà visualizzata la finestra di dialogo **Aggiornamenti di VirusScan** (Figura 3-16 a pagina 83). Fare clic su **Aggiorna** per continuare.

Se non è disponibile alcun aggiornamento, verrà visualizzata una finestra di dialogo per segnalare che VirusScan è aggiornato. Fare clic su **OK** per chiudere la finestra di dialogo.



Figura 3-16. Finestra di dialogo Aggiornamenti

4 Se richiesto, accedere al sito Web. La **procedura guidata di aggiornamento** consente di installare automaticamente l'aggiornamento.

5 Al termine dell'installazione dell'aggiornamento fare clic su **Fine**.

NOTA
In alcuni casi, verrà richiesto di riavviare il computer per completare l'aggiornamento. Prima di riavviare, assicurarsi di salvare tutti i dati e chiudere tutte le applicazioni.

McAfee Personal Firewall Plus 4

Benvenuti in McAfee Personal Firewall Plus.

Il software McAfee Personal Firewall Plus offre una protezione avanzata per il computer e per i dati personali. Personal Firewall consente di stabilire una barriera tra il computer in uso e Internet, monitorando il traffico Internet alla ricerca di attività sospette, senza richiedere interazione da parte dell'utente.

Grazie a questo software, è possibile usufruire delle seguenti funzioni:

- Difende dagli attacchi degli hacker
- Completa la difesa antivirus
- Controlla Internet e le attività della rete
- Segnala eventi potenzialmente dannosi
- Fornisce informazioni dettagliate sul traffico Internet sospetto
- Integra la funzionalità Hackerwatch.org, che include la creazione di segnalazioni sugli eventi, gli strumenti di test e la possibilità di inviare tramite posta elettronica gli eventi rilevati ad altre autorità online
- Fornisce funzioni dettagliate di ricerca e traccia degli eventi

Nuove funzioni

- **Supporto per i giochi potenziato**
  McAfee Personal Firewall Plus protegge il computer dai tentativi di intrusione e dalle attività sospette durante l'esecuzione di giochi a schermo intero, ma può nascondere gli avvisi se rileva tentativi di intrusione o attività sospette. Gli avvisi rossi vengono visualizzati dopo aver chiuso il gioco.
- **Gestione dell'accesso a Internet potenziata**
  McAfee Personal Firewall Plus consente agli utenti di concedere in modo dinamico alle applicazioni l'accesso temporaneo a Internet. L'accesso è limitato all'intervallo che intercorre tra quando viene avviata l'applicazione e quando viene chiusa. Se Personal Firewall rileva un programma sconosciuto che sta tentando di comunicare con Internet, un avviso rosso offre l'opzione di concedere all'applicazione l'accesso temporaneo a Internet.

- **Controllo della protezione potenziato**
  Se si esegue la funzione di blocco, McAfee Personal Firewall Plus consente di bloccare immediatamente tutto il traffico Internet in ingresso e in uscita tra il computer e Internet. Gli utenti possono attivare e disattivare il blocco direttamente da queste tre posizioni in Personal Firewall.

- **Opzioni di recupero potenziate**
  È possibile eseguire le **Opzioni di ripristino** per ripristinare automaticamente le impostazioni predefinite in Personal Firewall. Se Personal Firewall mostra un comportamento diverso da quello previsto, che non è possibile correggere, è possibile annullare le impostazioni correnti e tornare alle impostazioni predefinite del programma.

- **Protezione della connettività Internet**
  Per evitare che un utente disattivi inavvertitamente la connessione Internet, se Personal Firewall rileva una connessione Internet originata da un server DHCP o DNS, l'opzione di esclusione di un indirizzo Internet non viene inclusa negli avvisi blu. L'opzione viene visualizzata se il traffico in ingresso non viene originato da un server DHCP o DNS.

- **Integrazione con HackerWatch.org potenziata**
  La segnalazione di potenziali hacker è più facile che mai. McAfee Personal Firewall Plus migliora la funzionalità di HackerWatch.org, che comprende l'invio di eventi potenzialmente dannosi al database.

- **Gestione intelligente delle applicazioni estesa**
  Quando un'applicazione tenta di accedere a Internet, Personal Firewall verifica se è affidabile o dannosa. Se viene riconosciuta come affidabile, Personal Firewall ne consente automaticamente l'accesso a Internet, senza che sia necessario l'intervento dell'utente.

- **Rilevamento avanzato dei cavalli di Troia**
  McAfee Personal Firewall Plus combina la gestione delle connessioni delle applicazioni con un database potenziato per rilevare e bloccare l'accesso a Internet e la possibile ritrasmissione di dati personali da parte di più applicazioni potenzialmente dannose, come i cavalli di Troia.

- **Miglioramento di Visual Trace**
  Visual Trace comprende mappe grafiche intuitive che illustrano l'origine degli attacchi ostili e il traffico a livello mondiale, incluse informazioni dettagliate sul contatto/proprietario, a partire dagli indirizzi IP di origine.

- **Maggiore facilità d'uso**
  McAfee Personal Firewall Plus comprende un Assistente di installazione e un'Esercitazione per gli utenti che facilitano l'installazione e l'uso del firewall. Il prodotto è stato progettato per essere utilizzato senza alcun intervento, tuttavia McAfee offre una vasta gamma di risorse che permettono di capire e apprezzare le capacità del firewall.

- **Rilevamento delle intrusioni potenziato**
  Il Sistema di rilevamento intrusioni (IDS) di Personal Firewall rileva i più comuni tipi di attacco e altre attività sospette. Il rilevamento delle intrusioni controlla la presenza di trasferimenti di dati o metodi di trasferimento sospetti in ogni pacchetto di dati e li inserisce nel registro degli eventi.

- **Analisi del traffico potenziata**
  McAfee Personal Firewall Plus offre agli utenti una visualizzazione dei dati in ingresso e in uscita dei computer, nonché una visualizzazione delle connessioni delle applicazioni, comprese quelle di connessioni aperte che sono attivamente "in ascolto". In questo modo gli utenti possono vedere quali sono le applicazioni aperte a un'eventuale intrusione e intervenire di conseguenza.

Disinstallazione di altri firewall

Prima di installare il software McAfee Personal Firewall Plus, è necessario disinstallare eventuali altri programmi firewall presenti sul computer. Seguire le istruzioni di disinstallazione del programma firewall.

NOTA
Se si utilizza Windows XP, non è necessario disattivare il firewall incorporato prima di installare McAfee Personal Firewall Plus. Tuttavia, si consiglia di farlo. In caso contrario, non si riceveranno gli eventi nel registro Eventi in ingresso di McAfee Personal Firewall Plus.

Impostazione del firewall predefinito

McAfee Personal Firewall è in grado di gestire le autorizzazioni e il traffico per le applicazioni Internet presenti sul computer anche se Windows Firewall è in esecuzione.

Una volta installato, McAfee Personal Firewall disattiva automaticamente Windows Firewall e viene impostato come firewall predefinito. È quindi possibile utilizzare solo le funzionalità e i messaggi di McAfee Personal Firewall. Se in seguito si attiva Windows Firewall mediante Windows Security Center o il Pannello di controllo di Windows, l'esecuzione di entrambi i firewall sul computer potrebbe causare una parziale perdita di registrazione in McAfee Firewall, nonché la duplicazione di messaggi di stato e di avviso.

NOTA
Se sono attivati entrambi i firewall, McAfee Personal Firewall non mostra tutti gli indirizzi IP bloccati nella scheda **Eventi in ingresso**. Windows Firewall intercetta e blocca la maggior parte di questi eventi, impedendo a McAfee Personal Firewall di rilevarli o registrarli. McAfee Personal Firewall potrebbe tuttavia bloccare e registrare ulteriore traffico in base ad altri fattori di sicurezza.

In Windows Firewall la registrazione è disattivata per impostazione predefinita, ma se si attivano entrambi i firewall è possibile attivare tale registrazione. Il percorso del registro di Windows Firewall predefinito è C:\Windows\pfirewall.log.

Per garantire che il computer sia protetto da almeno un firewall, Windows Firewall viene automaticamente riattivato quando si disinstalla McAfee Personal Firewall.

Se si disattiva McAfee Personal Firewall o si imposta il livello di protezione su **Aperto** senza attivare manualmente Windows Firewall, l'intera protezione del firewall viene rimossa a eccezione delle applicazioni bloccate in precedenza.

Impostazione del livello di protezione

È possibile configurare le opzioni di protezione per indicare la modalità di risposta di Personal Firewall quando viene rilevato traffico indesiderato. Per impostazione predefinita, è attivato il livello di protezione **Standard**. Con il livello di protezione **Standard**, quando si consente a un'applicazione l'accesso a Internet, viene consentito l'accesso completo. L'accesso completo consente all'applicazione di inviare e ricevere dati non richiesti su porte non di sistema.

Per configurare le impostazioni di protezione:

1. Fare clic con il pulsante destro del mouse sull'icona McAfee nella barra delle applicazioni di Windows, scegliere **Personal Firewall**, quindi selezionare **Opzioni**.
2. Fare clic sull'icona **Impostazioni protezione**.

3 Impostare il livello di protezione desiderato utilizzando il dispositivo di scorrimento.

La gamma di livelli di protezione va da Blocco ad Aperto:

- **Blocco:** tutte le connessioni a Internet sul computer vengono chiuse. È possibile utilizzarla per bloccare porte configurate come aperte nella pagina **Servizi di sistema**.
- **Protezione elevata:** se un'applicazione richiede solo un tipo di accesso a Internet specifico (ad esempio Solo accesso in uscita), è possibile concedere o meno una connessione Internet all'applicazione. Se in seguito l'applicazione richiede l'accesso completo, è possibile concederlo o mantenere solo l'accesso in uscita.
- **Protezione standard (impostazione consigliata):** se un'applicazione richiede l'accesso a Internet e questo le viene concesso, viene consentito l'accesso completo per gestire il traffico in ingresso e in uscita.
- **Protezione basata sull'affidabilità:** tutte le applicazioni vengono automaticamente ritenute affidabili al primo tentativo di accesso a Internet. È tuttavia possibile configurare Personal Firewall in modo da poter utilizzare gli avvisi per la notifica di nuove applicazioni sul computer. Utilizzare questa impostazione in caso di mancato funzionamento di alcuni giochi o dello streaming audio o video.
- **Aperto:** il firewall è disattivato. Questa impostazione consente il passaggio di tutto il traffico attraverso Personal Firewall senza alcun filtro.

  NOTA
  Quando il livello di protezione del firewall è impostato su **Aperto** o **Blocco**, le applicazioni bloccate in precedenza continuano a essere bloccate. Per impedire che ciò si verifichi, è possibile impostare le autorizzazioni dell'applicazione su **Accesso completo** oppure eliminare la regola di autorizzazione **Blocco** nell'elenco **Applicazioni Internet**.

4 Selezionare ulteriori impostazioni di protezione:

  NOTA
  Se si utilizza Windows XP e sono stati aggiunti più utenti di XP, le opzioni riportate di seguito sono disponibili solo se si accede al computer in qualità di amministratore.

- **Registra eventi di Sistema di rilevamento intrusioni (IDS) nel registro Eventi in ingresso:** se si seleziona questa opzione, gli eventi rilevati da IDS vengono visualizzati nel registro Eventi in ingresso. Il Sistema di rilevamento delle intrusioni rileva i tipi di attacco comuni e altre attività sospette. Il rilevamento delle intrusioni verifica tutti i pacchetti di dati in ingresso e in uscita alla ricerca di trasferimenti di dati o metodi di trasferimento sospetti, li confronta con un database di firme ed esclude automaticamente quelli provenienti dal computer che genera l'attacco.

IDS cerca specifici modelli di traffico utilizzati dagli hacker. IDS verifica tutti i pacchetti ricevuti dal computer alla ricerca di traffico sospetto o attacchi noti. Ad esempio, se in Personal Firewall vengono visualizzati i pacchetti ICMP, tali pacchetti vengono analizzati alla ricerca di modelli di traffico sospetti confrontando il traffico ICMP con modelli di attacco noti.

- **Accetta richieste ping ICMP**: il traffico ICMP viene utilizzato principalmente per l'esecuzione di tracce e ping. Il ping viene spesso utilizzato per eseguire una rapida verifica prima di tentare di stabilire le comunicazioni. Se si utilizza o si è utilizzato un programma di condivisione di file peer-to-peer, è possibile che si riceva un numero elevato di ping. Se si seleziona questa opzione, Personal Firewall consente tutte le richieste di ping senza registrare i ping nel registro Eventi in ingresso. Se l'opzione non è selezionata, Personal Firewall blocca tutte le richieste di ping e registra i ping nel registro Eventi in ingresso.
- **Consenti a utenti con restrizioni di modificare impostazioni di Personal Firewall**: se si utilizza Windows XP o Windows 2000 Professional con più utenti, selezionare questa opzione per consentire agli utenti XP con restrizioni di modificare le impostazioni di Personal Firewall.

5 Dopo aver apportato le modifiche desiderate, fare clic su **OK**.

Verifica di McAfee Personal Firewall Plus

È possibile verificare l'installazione di Personal Firewall per controllarne la possibile vulnerabilità a intrusioni e attività sospette.

Per verificare l'installazione di Personal Firewall dall'icona McAfee visualizzata nella barra delle applicazioni:

- Fare clic con il pulsante destro del mouse sull'icona McAfee nella barra delle applicazioni di Windows e selezionare **Prova firewall**.

Personal Firewall apre Internet Explorer e all'indirizzo http://www.hackerwatch.org/ viene visualizzato il sito Web di HackerWatch gestito da McAfee. Per verificare Personal Firewall, seguire le istruzioni visualizzate nell'apposita pagina di Hackerwatch.org.

Utilizzo di McAfee Personal Firewall Plus

Per aprire Personal Firewall:

- Fare clic con il pulsante destro del mouse sull'icona McAfee nella barra delle applicazioni di Windows, scegliere **Personal Firewall**, quindi selezionare un'attività.

Informazioni sulla pagina Riepilogo

Il riepilogo di Personal Firewall comprende quattro pagine riassuntive:

- Riepilogo principale
- Riepilogo applicazione
- Riepilogo eventi
- Riepilogo di HackerWatch

Le pagine **Riepilogo** contengono una grande varietà di segnalazioni sugli eventi recenti in ingresso, sullo stato delle applicazioni e sulle attività di intrusione in tutto il mondo segnalate da HackerWatch.org, nonché collegamenti alle operazioni più comuni eseguite in Personal Firewall.

Per aprire la pagina **Riepilogo principale** in Personal Firewall:

- Fare clic con il pulsante destro del mouse sull'icona McAfee nella barra delle applicazioni di Windows, scegliere **Personal Firewall**, quindi selezionare **Visualizza riepilogo** (Figura 4-1).



Figura 4-1. Pagina Riepilogo principale

Fare clic sulle seguenti opzioni per accedere alle varie pagine Riepilogo:

Voce	Descrizione
Modifica visualizzazione	Fare clic su **Modifica visualizzazione** per aprire un elenco di pagine Riepilogo. Nell'elenco selezionare una pagina Riepilogo da visualizzare.
Freccia destra	Fare clic sull'icona a forma di freccia rivolta verso destra per visualizzare la pagina Riepilogo successiva.
Freccia sinistra	Fare clic sull'icona a forma di freccia rivolta verso sinistra per visualizzare la pagina Riepilogo precedente.
Home Page	Fare clic sull'icona della home page per tornare alla pagina **Riepilogo principale**.

Nella pagina **Riepilogo principale** sono disponibili le seguenti informazioni:

Voce	Descrizione
Impostazione di protezione	Lo stato dell'impostazione di protezione indica il livello di protezione su cui è impostato il firewall. Fare clic sul collegamento per modificare il livello di protezione.
Eventi bloccati	Lo stato eventi bloccati visualizza il numero di eventi bloccati nel corso della giornata. Fare clic sul collegamento per visualizzarne i dettagli provenienti dalla pagina **Eventi in ingresso**.
Modifiche regole applicazioni	Lo stato della regola dell'applicazione visualizza il numero di regole applicazioni che sono state modificate di recente. Fare clic sul collegamento per visualizzare l'elenco di applicazioni consentite e bloccate nonché per modificare le autorizzazioni delle applicazioni.
Novità	**Novità** in quest'area viene mostrata l'ultima applicazione a cui è stato consentito accesso completo a Internet.
Ultimo evento	**Ultimo evento** visualizza gli eventi in ingresso più recenti. È possibile fare clic su un collegamento per rintracciare l'evento o per impostare l'indirizzo IP come affidabile. Se si imposta un indirizzo IP come affidabile, si consente a tutto il traffico che ne proviene di raggiungere il computer.
Rapporto giornaliero	**Rapporto giornaliero** visualizza il numero di eventi in ingresso bloccati da Personal Firewall durante la giornata, la settimana e il mese in corso. Fare clic sul collegamento per visualizzarne i dettagli provenienti dalla pagina **Eventi in ingresso**.

Voce	Descrizione
Applicazioni attive	**Applicazioni attive** visualizza le applicazioni attualmente in esecuzione nel computer e connesse a Internet. Fare clic su un'applicazione per visualizzare gli indirizzi IP a cui l'applicazione è connessa.
Attività comuni	Fare clic su un collegamento nell'area **Attività comuni** per andare alle pagine di Personal Firewall in cui è possibile visualizzare l'attività del firewall ed eseguire le attività.

Per visualizzare la pagina **Riepilogo applicazione**:

1. Fare clic con il pulsante destro del mouse sull'icona McAfee nella barra delle applicazioni di Windows, scegliere **Personal Firewall**, quindi selezionare **Visualizza riepilogo**.
2. Fare clic su **Modifica visualizzazione**, quindi selezionare **Riepilogo applicazione**.

Nella pagina **Riepilogo applicazione** sono disponibili le seguenti informazioni:

Voce	Descrizione
Controllo traffico	**Controllo traffico** visualizza le connessioni Internet in ingresso e in uscita nel corso degli ultimi quindici minuti. Fare clic sul grafico per visualizzare i dettagli di controllo del traffico.
Applicazioni attive	**Applicazioni attive** visualizza l'utilizzo della larghezza di banda delle applicazioni più attive del computer nel corso delle ultime 24 ore. **Applicazione**: l'applicazione che accede a Internet. **%**: la percentuale di larghezza di banda utilizzata dall'applicazione. **Autorizzazione**: il tipo di accesso a Internet consentito all'applicazione. **Regola creata**: data e ora di creazione della regola per l'applicazione.
Novità	**Novità** in quest'area viene mostrata l'ultima applicazione a cui è stato consentito accesso completo a Internet.
Applicazioni attive	**Applicazioni attive** visualizza le applicazioni attualmente in esecuzione nel computer e connesse a Internet. Fare clic su un'applicazione per visualizzare gli indirizzi IP a cui l'applicazione è connessa.
Attività comuni	Fare clic su un collegamento nell'area **Attività comuni** per andare alle pagine di Personal Firewall in cui è possibile vedere lo stato dell'applicazione ed eseguire attività relative all'applicazione.

Per visualizzare la pagina **Riepilogo eventi**:

1. Fare clic con il pulsante destro del mouse sull'icona McAfee nella barra delle applicazioni di Windows, scegliere **Personal Firewall**, quindi selezionare **Visualizza riepilogo**.
2. Fare clic su **Modifica visualizzazione**, quindi selezionare **Riepilogo eventi**.

Nella pagina **Riepilogo eventi** sono disponibili le seguenti informazioni:

Voce	Descrizione
Confronto porte	**Confronto porte** visualizza un grafico a torta relativo alle porte del computer in uso su cui è stato effettuato il maggior numero di tentativi nel corso degli ultimi 30 giorni. È possibile fare clic sul nome di una porta per visualizzarne i dettagli provenienti dalla pagina **Eventi in ingresso**. È inoltre possibile spostare il puntatore del mouse sul numero di una porta per visualizzarne una descrizione.
Principali eventi	**Principali eventi** visualizza gli indirizzi IP bloccati più di frequente, la data e l'ora in cui si è verificato l'ultimo evento in ingresso per ogni indirizzo e il numero totale di eventi in ingresso nel corso degli ultimi trenta giorni per ogni indirizzo. Fare clic su un evento per visualizzarne i dettagli provenienti dalla pagina **Eventi in ingresso**.
Rapporto giornaliero	**Rapporto giornaliero** visualizza il numero di eventi in ingresso bloccati da Personal Firewall durante la giornata, la settimana e il mese in corso. Fare clic su un numero per visualizzare i dettagli dell'evento provenienti dalla pagina Eventi in ingresso.
Ultimo evento	**Ultimo evento** visualizza gli eventi in ingresso più recenti. È possibile fare clic su un collegamento per rintracciare l'evento o per impostare l'indirizzo IP come affidabile. Se si imposta un indirizzo IP come affidabile, si consente a tutto il traffico che ne proviene di raggiungere il computer.
Attività comuni	Fare clic su un collegamento nell'area **Attività comuni** per accedere alle pagine di Personal Firewall in cui è possibile visualizzare i dettagli degli eventi ed eseguire attività relative agli eventi.

Per visualizzare la pagina **Riepilogo di HackerWatch**:

1. Fare clic con il pulsante destro del mouse sull'icona McAfee nella barra delle applicazioni di Windows, scegliere **Personal Firewall**, quindi selezionare **Visualizza riepilogo**.
2. Fare clic su **Modifica visualizzazione**, quindi selezionare **Riepilogo di HackerWatch**.

Nella pagina **Riepilogo di HackerWatch** sono disponibili le informazioni seguenti.

Voce	Descrizione
Attività a livello mondiale	**Attività a livello mondiale** in quest'area viene visualizzata una mappa mondiale in cui sono identificate le attività bloccate di recente controllate da HackerWatch.org. Fare clic sulla mappa per aprire la mappa di Analisi delle minacce globali in HackerWatch.org.
Traccia degli eventi	**Traccia degli eventi** visualizza il numero di eventi in ingresso inviati a HackerWatch.org.
Attività globale delle porte	**Attività globale delle porte** visualizza le porte principali che sono state minacciate nel corso degli ultimi cinque giorni. Fare clic su una porta per visualizzarne il numero e la descrizione.
Attività comuni	Fare clic su un collegamento nell'area **Attività comuni** per accedere alle pagine di HackerWatch.org in cui è possibile ottenere ulteriori informazioni sulle attività degli hacker in tutto il mondo.

Informazioni sulla pagina Applicazioni Internet

Nella pagina **Applicazioni Internet** viene visualizzato l'elenco delle applicazioni autorizzate e bloccate.

Per avviare la pagina **Applicazioni Internet**:

- Fare clic con il pulsante destro del mouse sull'icona McAfee nella barra delle applicazioni di Windows, scegliere **Personal Firewall**, quindi selezionare **Applicazioni** (Figura 4-2).

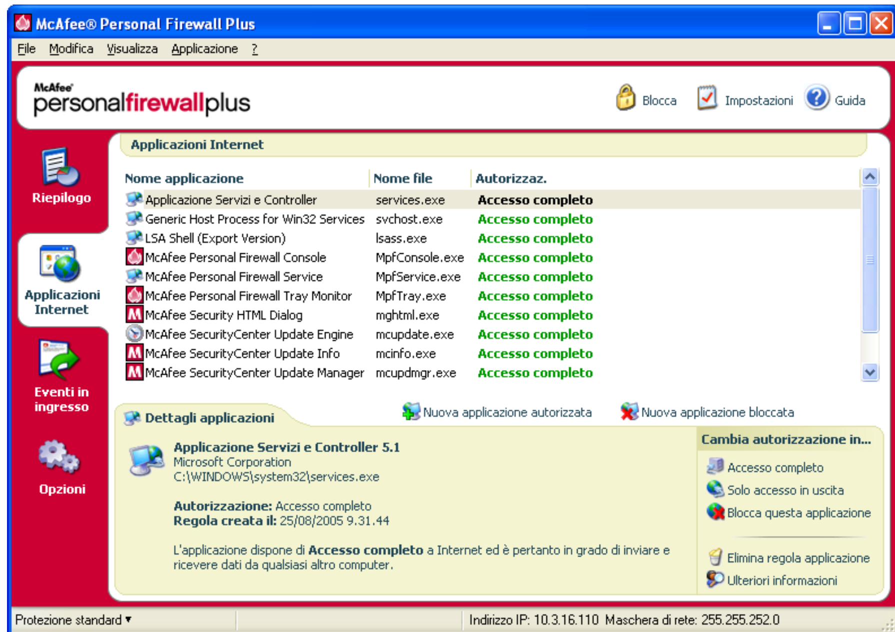


Figura 4-2. Pagina Applicazioni Internet

Nella pagina **Applicazioni Internet** sono disponibili le seguenti informazioni:

- Nomi delle applicazioni
- Nomi dei file
- Livelli di autorizzazione correnti
- Dettagli sulle applicazioni: nome e versione dell'applicazione, nome della società, nome del percorso, timestamp e spiegazione dei tipi di autorizzazione

Modifica delle regole delle applicazioni

Personal Firewall consente di modificare le regole di accesso per le applicazioni.

Per modificare la regola di un'applicazione:

1 Fare clic con il pulsante destro del mouse sull'icona McAfee, scegliere **Personal Firewall**, quindi selezionare **Applicazioni Internet**.

2 Nell'elenco **Applicazioni Internet**, fare clic con il pulsante destro del mouse sulla regola di un'applicazione e selezionare un livello diverso:

- **Accesso completo:** consente all'applicazione di stabilire connessioni Internet in uscita e in ingresso.
- **Solo accesso in uscita:** consente all'applicazione di stabilire solo una connessione Internet in uscita.
- **Blocca questa applicazione:** non consente all'applicazione di accedere a Internet.

NOTA
Quando il firewall è impostato su **Aperto** o **Blocco**, le applicazioni bloccate in precedenza continuano a essere bloccate. Per impedire che ciò si verifichi, è possibile impostare la regola di accesso dell'applicazione su **Accesso completo** oppure eliminare la regola di autorizzazione **Blocco** nell'elenco **Applicazioni Internet**.

Per eliminare la regola di un'applicazione:

1 Fare clic con il pulsante destro del mouse sull'icona McAfee nella barra delle applicazioni di Windows, scegliere **Personal Firewall**, quindi selezionare **Applicazioni Internet**.

2 Nell'elenco **Applicazioni Internet**, fare clic con il pulsante destro del mouse sulla regola dell'applicazione, quindi selezionare **Eliminare regola applicazione**.

Alla successiva richiesta di accesso a Internet da parte dell'applicazione, sarà possibile impostarne il livello di autorizzazione per aggiungerla nuovamente all'elenco.

Autorizzazione e blocco delle applicazioni Internet

Per modificare l'elenco delle applicazioni Internet autorizzate e bloccate:

1 Fare clic con il pulsante destro del mouse sull'icona McAfee nella barra delle applicazioni di Windows, scegliere **Personal Firewall**, quindi selezionare **Applicazioni Internet**.

2 Nella pagina **Applicazioni Internet**, fare clic su una delle seguenti opzioni:

- **Nuova applicazione autorizzata**: consente all'applicazione l'accesso completo a Internet.
- **Nuova applicazione bloccata**: non consente all'applicazione di accedere a Internet.
- **Eliminare regola applicazione**: consente di rimuovere la regola di un'applicazione.

Informazioni sulla pagina Eventi in ingresso

Utilizzare la pagina **Eventi in ingresso** per visualizzare il registro Eventi in ingresso generato quando le connessioni Internet non richieste vengono bloccate da Personal Firewall.

Per aprire la pagina **Eventi in ingresso**:

- Fare clic con il pulsante destro del mouse sull'icona McAfee nella barra delle applicazioni di Windows, scegliere **Personal Firewall**, quindi selezionare **Eventi in ingresso** (Figura 4-3).

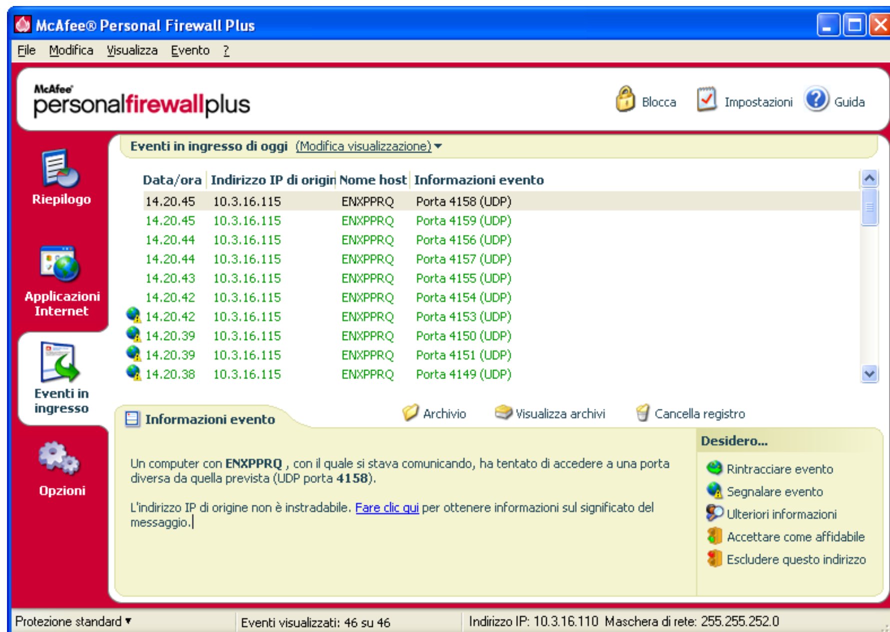


Figura 4-3. Pagina Eventi in ingresso

Nella pagina **Eventi in ingresso** sono disponibili le seguenti informazioni:

- Timestamp
- Indirizzi IP di origine
- Nomi host
- Nomi del servizio o dell'applicazione
- Dettagli eventi: tipi di connessione, porte di connessione, nome host o IP e spiegazione del significato degli eventi relativi alle varie porte

Informazioni sugli eventi

Informazioni sugli indirizzi IP

Gli indirizzi IP sono numeri. Per la precisione, sono costituiti da quattro numeri compresi tra 0 e 255. Tali numeri indicano una destinazione precisa a cui può essere indirizzato il traffico su Internet.

I tipi di indirizzi IP

Numerosi indirizzi IP sono considerati speciali per varie ragioni:

Indirizzi IP non instradabili: tali indirizzi sono noti anche come "spazi IP privati" e non possono essere utilizzati su Internet. I blocchi privati sono 10.x.x.x, 172.16.x.x - 172.31.x.x e 192.168.x.x.

Indirizzi IP di loop-back: gli indirizzi di loop-back vengono utilizzati a scopo di test. Il traffico inviato a questo blocco di indirizzi IP torna subito al dispositivo che genera il pacchetto, non lascia mai il dispositivo e viene utilizzato principalmente per test di hardware e software. Il blocco di indirizzi IP di loop-back è 127.x.x.x.

Indirizzo IP nullo: indirizzo non valido. Una volta rilevato, Personal Firewall indica che il traffico utilizzava un indirizzo IP vuoto. Spesso questa situazione indica che l'origine del traffico viene deliberatamente nascosta dal mittente. Il mittente non sarà in grado di ricevere risposte al traffico, a meno che il pacchetto non venga ricevuto da un'applicazione in grado di comprendere i contenuti del pacchetto in cui sono incluse istruzioni specifiche per tale applicazione. Qualsiasi indirizzo che inizi per 0 (0.x.x.x) è un indirizzo nullo. Ad esempio, 0.0.0.0 è un indirizzo IP nullo.

Eventi da 0.0.0.0

Due sono le cause più probabili per il rilevamento di eventi dall'indirizzo IP 0.0.0.0. La prima causa, più comune, è che il computer abbia ricevuto un pacchetto non corretto. Internet non è sempre affidabile al 100% ed è possibile che vengano inoltrati pacchetti non validi. Poiché i pacchetti vengono esaminati da Personal Firewall prima della convalida da parte di TCP/IP, è possibile che vengano segnalati come evento.

Nel secondo caso, l'indirizzo IP di origine ha subito un attacco di tipo spoofing, ovvero è stato contraffatto. I pacchetti contraffatti possono indicare la scansione in corso del computer alla ricerca di cavalli di Troia. Personal Firewall blocca questo tipo di attività, quindi il computer in uso è sicuro.

Eventi da 127.0.0.1

Alcuni eventi vengono generati dall'indirizzo IP 127.0.0.1. Questo viene chiamato indirizzo di loopback o localhost.

Molti programmi legittimi utilizzano infatti l'indirizzo di loopback per la comunicazione fra i componenti. Ad esempio, è possibile configurare molti server di posta elettronica o Web tramite un'interfaccia Web. Per accedere all'interfaccia, digitare http://localhost/ nel browser Web.

Il traffico proveniente da tali programmi viene autorizzato da Personal Firewall, quindi se si rilevano eventi da 127.0.0.1, è probabile che l'indirizzo IP di origine sia stato sottoposto a spoofing, ovvero sia stato contraffatto. I pacchetti contraffatti indicano in genere che un altro computer sta eseguendo la scansione del proprio computer alla ricerca di cavalli di Troia. Personal Firewall blocca questi tentativi di intrusione, quindi il computer in uso è sicuro.

Esistono programmi, come Netscape 6.2 e versioni successive, che richiedono l'aggiunta di 127.0.0.1 all'elenco **Indirizzi IP affidabili**. La modalità di comunicazione tra i componenti di tali programmi non consente a Personal Firewall di determinare se si tratti o meno di traffico locale.

Nel caso di Netscape 6.2, se non si imposta 127.0.0.1 come affidabile, non sarà possibile utilizzare l'elenco degli amici. Se si rileva quindi traffico proveniente da 127.0.0.1 e tutte le applicazioni del computer funzionano normalmente, è possibile bloccare tale traffico senza che si verifichino problemi. Se tuttavia in un programma, ad esempio Netscape, si verificano problemi, aggiungere 127.0.0.1 all'elenco **Indirizzi IP affidabili** di Personal Firewall, quindi verificare se i problemi sono stati risolti.

Se l'inserimento di 127.0.0.1 nell'elenco degli indirizzi IP affidabili consente di risolvere il problema, è necessario valutare attentamente le opzioni disponibili. Se si imposta 127.0.0.1 come affidabile, il programma funzionerà correttamente, ma il sistema sarà più vulnerabile ad attacchi di spoofing. Se non si ritiene affidabile l'indirizzo, il programma non funzionerà correttamente, ma il sistema sarà protetto dal traffico dannoso.

Eventi dai computer nella LAN

Gli eventi possono essere generati dai computer presenti nella LAN. Questi eventi vengono visualizzati in verde, a indicare che provengono dalla rete.

Nella maggior parte delle configurazioni LAN aziendali si consiglia di selezionare la casella di controllo **Considera affidabili tutti i computer della LAN** nella finestra di dialogo **Indirizzi IP affidabili**.

In determinate situazioni, la rete "locale" può essere tanto pericolosa quanto Internet, soprattutto se si utilizza una rete DSL o con modem via cavo a larghezza di banda elevata. In tal caso, è consigliabile non selezionare l'opzione **Considera affidabili tutti i computer della LAN**. Aggiungere, invece, gli indirizzi IP dei computer locali all'elenco **Indirizzi IP affidabili**.

Eventi dagli indirizzi IP privati

Gli indirizzi IP con formato 192.168.xxx.xxx, 10.xxx.xxx.xxx e 172.16.0.0 - 172.31.255.255 sono detti non instradabili o privati. Tali indirizzi IP non dovrebbero mai lasciare la rete e possono essere considerati quasi sempre affidabili.

Il blocco 192.168 xxx.xxx viene utilizzato con Condivisione connessione Internet di Microsoft (ICS). Se si utilizza Condivisione connessione Internet e si rilevano eventi provenienti da tale blocco IP, è possibile aggiungere l'indirizzo IP 192.168.255.255 all'elenco **Indirizzi IP affidabili**. In tal modo verrà impostato come affidabile l'intero blocco 192.168.xxx.xxx.

Se non si è connessi a una rete privata e si rilevano eventi provenienti da tali intervalli IP, è possibile che gli indirizzi IP di origine siano stati sottoposti a spoofing, ovvero siano stati contraffatti. I pacchetti contraffatti indicano in genere una scansione per la ricerca di cavalli di Troia. È importante ricordare che tale tentativo è stato bloccato da Personal Firewall, quindi il computer in uso è sicuro.

Poiché gli indirizzi IP privati fanno riferimento a computer diversi a seconda della rete a cui si è connessi, la segnalazione di tali eventi risulta inutile, quindi non viene effettuata.

Visualizzazione degli eventi nel registro Eventi in ingresso

Nel registro Eventi in ingresso, gli eventi vengono visualizzati in numerosi modi diversi. La visualizzazione predefinita mostra solo gli eventi che si verificano nel corso della giornata. È possibile visualizzare anche gli eventi che si sono verificati durante la settimana scorsa oppure il registro completo.

Grazie a Personal Firewall è inoltre possibile visualizzare eventi in ingresso relativi a giorni specifici, provenienti da specifici indirizzi Internet (indirizzi IP) o contenenti le stesse informazioni sull'evento.

Per informazioni su un evento, fare clic sull'evento. Le informazioni verranno visualizzate nel riquadro **Informazioni evento**.

Visualizzazione degli eventi odierni

Utilizzare questa opzione per rivedere gli eventi odierni.

Per visualizzare gli eventi odierni:

1 Fare clic con il pulsante destro del mouse sull'icona McAfee nella barra delle applicazioni di Windows, scegliere **Personal Firewall**, quindi selezionare **Eventi in ingresso**.

2 Nel registro degli eventi in ingresso, fare clic con il pulsante destro del mouse su una voce, quindi fare clic su **Mostra eventi di oggi**.

Visualizzazione degli eventi della settimana

Utilizzare questa opzione per rivedere gli eventi settimanali.

Per visualizzare gli eventi della settimana:

1 Fare clic con il pulsante destro del mouse sull'icona McAfee nella barra delle applicazioni di Windows, scegliere **Personal Firewall**, quindi selezionare **Eventi in ingresso**.

2 Nel registro degli eventi in ingresso, fare clic con il pulsante destro del mouse su una voce, quindi fare clic su **Mostra eventi di questa settimana**.

Visualizzazione del registro Eventi in ingresso completo

Utilizzare questa opzione per rivedere tutti gli eventi.

Per visualizzare tutti gli eventi nel registro Eventi in ingresso:

1 Fare clic con il pulsante destro del mouse sull'icona McAfee, scegliere **Personal Firewall**, quindi fare clic su **Eventi in ingresso**.

2 Nel registro degli eventi in ingresso, fare clic con il pulsante destro del mouse su una voce, quindi fare clic su **Mostra registro completo**.

   Il registro degli eventi in ingresso visualizza tutti gli eventi del registro.

Visualizzazione degli eventi di un giorno specifico

Utilizzare questa opzione per rivedere gli eventi di un giorno specifico.

Per visualizzare gli eventi di un giorno specifico:

1 Fare clic con il pulsante destro del mouse sull'icona McAfee nella barra delle applicazioni di Windows, scegliere **Personal Firewall**, quindi selezionare **Eventi in ingresso**.

2 Nel registro degli eventi in ingresso, fare clic con il pulsante destro del mouse su una voce, quindi fare clic su **Mostra solo eventi del giorno selezionato**.

Visualizzazione degli eventi da un indirizzo Internet specifico

Utilizzare questa opzione per rivedere gli eventi che vengono originati da un particolare indirizzo Internet.

Per visualizzare gli eventi di un indirizzo Internet:

1. Fare clic con il pulsante destro del mouse sull'icona McAfee nella barra delle applicazioni di Windows, scegliere **Personal Firewall** e fare clic su **Eventi in ingresso**.
2. Nel registro degli eventi in ingresso, fare clic con il pulsante destro del mouse su una voce, quindi fare clic su **Mostra solo eventi dell'indirizzo Internet selezionato**.

Visualizzazione di eventi con le stesse informazioni sull'evento

Utilizzare questa opzione per rivedere gli eventi nel registro degli eventi in ingresso per i quali nella colonna **Informazioni evento** sono riportate le stesse informazioni dell'evento selezionato. È possibile verificare quante volte si è verificato l'evento e se proviene dalla stessa origine. La colonna **Informazioni evento** contiene una descrizione dell'evento e, se noto, il programma o il servizio comune che utilizza la porta interessata.

Per visualizzare gli eventi con le stesse informazioni sull'evento:

1. Fare clic con il pulsante destro del mouse sull'icona McAfee nella barra delle applicazioni di Windows, scegliere **Personal Firewall** e fare clic su **Eventi in ingresso**.
2. Nel registro degli eventi in ingresso, fare clic con il pulsante destro del mouse su una voce, quindi fare clic su **Mostra solo eventi con le stesse informazioni sull'evento**.

Risposta agli eventi in ingresso

Oltre a rivedere informazioni dettagliate sugli eventi visualizzati nel registro Eventi in ingresso, è possibile creare con Visual Trace una traccia degli indirizzi IP di un evento del registro Eventi in ingresso oppure ottenere informazioni sull'evento visitando HackerWatch.org, il sito Web della comunità online per la protezione dagli attacchi degli hacker.

Traccia dell'evento selezionato

È possibile tentare di creare con Visual Trace una traccia visuale degli indirizzi IP relativi a un evento riportato nel registro Eventi in ingresso.

Per creare la traccia di un evento selezionato:

1 Fare clic con il pulsante destro del mouse sull'icona McAfee nella barra delle applicazioni di Windows, scegliere **Personal Firewall** e selezionare **Eventi in ingresso**.

2 Nel registro eventi in ingresso, fare clic con il pulsante destro del mouse sull'evento che si desidera rintracciare, quindi scegliere **Rintraccia evento selezionato**. Per tenere traccia di un evento è possibile anche fare doppio clic su un evento.

Per impostazione predefinita, la traccia visuale viene avviata in Personal Firewall mediante il programma Visual Trace di Personal Firewall.

Suggerimenti da HackerWatch.org

Per ottenere suggerimenti da HackerWatch.org:

1 Fare clic con il pulsante destro del mouse sull'icona McAfee, scegliere **Personal Firewall** e selezionare **Eventi in ingresso**.

2 Selezionare l'evento nella pagina **Eventi in ingresso**, quindi fare clic su **Ulteriori informazioni** nel riquadro **Desidero**.

Il browser Web predefinito verrà aperto e verrà visualizzato il sito Web HackerWatch.org in cui sono disponibili informazioni relative al tipo di evento e suggerimenti relativi all'opportunità di segnalare l'evento.

Segnalazione di un evento

Per segnalare un evento che si ritiene essere un attacco al computer in uso:

1 Fare clic con il pulsante destro del mouse sull'icona McAfee nella barra delle applicazioni di Windows, scegliere **Personal Firewall** e selezionare **Eventi in ingresso**.

2 Fare clic sull'evento che si desidera segnalare, quindi fare clic su **Segnalare evento** nel riquadro **Desidero**.

Personal Firewall segnala l'evento al sito Web HackerWatch.org, utilizzando l'ID univoco del computer in uso.

Registrazione a HackerWatch.org

Alla prima apertura della pagina **Riepilogo**, HackerWatch.org verrà contattato da Personal Firewall per generare un ID utente univoco. Se si è già utenti registrati, la richiesta di accesso verrà convalidata automaticamente. Ai nuovi utenti viene richiesta l'immissione di uno pseudonimo e di un indirizzo di posta elettronica. Per utilizzare le funzionalità di filtro e di invio tramite posta elettronica degli eventi disponibili nel sito Web sarà quindi necessario fare clic sul collegamento di convalida disponibile nel messaggio di posta elettronica di conferma di HackerWatch.org.

È possibile segnalare eventi a HackerWatch.org senza convalidare l'ID utente. Per filtrare e inviare tramite posta elettronica degli eventi a un amico è tuttavia necessario effettuare la registrazione al servizio.

L'abbonamento a tale servizio consente di tenere traccia delle segnalazioni inviate e di ricevere avvisi, nel caso in cui a HackerWatch.org siano necessarie più informazioni o ulteriori azioni da parte dell'utente. L'abbonamento consente inoltre di verificare tutte le informazioni ricevute, in modo da poterle utilizzare.

Tutti gli indirizzi di posta elettronica forniti a HackerWatch.org rimangono riservati. Se una richiesta di ulteriori informazioni viene inviata da un ISP, tale richiesta viene reindirizzata tramite HackerWatch.org, in modo da non esporre mai l'indirizzo di posta elettronica degli utenti.

Considerare affidabile un indirizzo

È possibile utilizzare la pagina **Eventi in ingresso** per aggiungere un indirizzo IP all'elenco **Indirizzi IP affidabili** e consentire una connessione permanente.

Se nella pagina **Eventi in ingresso** viene individuato un evento contenente un indirizzo IP che si desidera autorizzare, è possibile impostare Personal Firewall in modo che le connessioni da tale indirizzo siano consentite in qualunque momento.

Per aggiungere un indirizzo IP all'elenco **Indirizzi IP affidabili**:

1. Fare clic con il pulsante destro del mouse sull'icona McAfee nella barra delle applicazioni di Windows, scegliere **Personal Firewall** e selezionare **Eventi in ingresso**.
2. Fare clic con il pulsante destro del mouse sull'evento contenente l'indirizzo IP da impostare come affidabile e scegliere **Considera affidabile l'indirizzo IP di origine**.

Verificare che l'indirizzo IP visualizzato nella finestra di dialogo **Considerare affidabile questo indirizzo** sia corretto, quindi fare clic su **OK**. L'indirizzo IP verrà aggiunto all'elenco **Indirizzi IP affidabili**.

Per assicurarsi che l'indirizzo IP sia stato aggiunto:

1. Fare clic con il pulsante destro del mouse sull'icona McAfee nella barra delle applicazioni di Windows, scegliere **Personal Firewall** e selezionare **Opzioni**.
2. Fare clic sull'icona **IP affidabili ed esclusi**, quindi sulla scheda **Indirizzi IP affidabili**.

L'indirizzo IP verrà visualizzato nell'elenco **Indirizzi IP affidabili**.

Esclusione di un indirizzo

Se nel registro eventi in ingresso viene visualizzato un indirizzo IP, questo significa che il traffico proveniente da tale indirizzo è stato bloccato. Pertanto, l'esclusione di un indirizzo non aggiunge ulteriore protezione a meno che il computer non abbia porte deliberatamente aperte dalla funzione Servizi di sistema o un'applicazione autorizzata a ricevere dati.

Aggiungere un indirizzo IP all'elenco di esclusione solo se si dispone di una o più porte deliberatamente aperte e se si ha motivo di credere che sia necessario bloccarle.

Se nella pagina **Eventi in ingresso** viene individuato un evento contenente un indirizzo IP che si desidera escludere, è possibile configurare Personal Firewall in modo che le connessioni da tale indirizzo non siano mai consentite.

È possibile utilizzare la pagina **Eventi in ingresso**, che elenca gli indirizzi IP del traffico Internet in ingresso, per escludere un indirizzo IP che sembra essere l'origine di attività Internet sospette o indesiderate.

Per aggiungere un indirizzo IP all'elenco **Indirizzi IP esclusi**:

1. Fare clic con il pulsante destro del mouse sull'icona McAfee nella barra delle applicazioni di Windows, scegliere **Personal Firewall**, quindi selezionare **Eventi in ingresso**.
2. La pagina **Eventi in ingresso** elenca gli indirizzi IP del traffico Internet in ingresso. Selezionare un indirizzo IP, quindi eseguire una delle seguenti operazioni:
   - Fare clic con il pulsante destro del mouse sull'indirizzo IP, quindi selezionare **Escludi l'indirizzo IP di origine**.
   - Fare clic su **Escludere questo indirizzo** nel menu **Desidero**.
3. Nella finestra di dialogo **Aggiungi regola indirizzi IP esclusi**, utilizzare una o più impostazioni seguenti per configurare la regola dell'indirizzo IP escluso:
   - **Indirizzo IP singolo**: l'indirizzo IP da escludere. L'indirizzo predefinito è quello selezionato nella pagina **Eventi in ingresso**.
   - **Intervallo di indirizzi IP**: gli indirizzi IP tra l'indirizzo specificato in **Da indirizzo IP** e l'indirizzo specificato in **A indirizzo IP**.

- **Data scadenza regola**: data e ora in cui la regola dell'indirizzo IP escluso scade. Per selezionare la data e l'ora, selezionare i menu a discesa appropriati.
- **Descrizione**: se lo si desidera, descrivere la nuova regola.
- Fare clic su **OK**.

4 Nella finestra di dialogo, fare clic su **Sì** per confermare l'impostazione. Fare clic su **No** per tornare alla finestra di dialogo **Aggiungi regola indirizzi IP esclusi**.

Se viene rilevato un evento proveniente da una connessione Internet esclusa, verrà inviato un avviso in base al metodo specificato nella pagina **Impostazioni avviso**.

Per assicurarsi che l'indirizzo IP sia stato aggiunto:

1. Fare clic sulla scheda **Opzioni**.
2. Fare clic sull'icona **IP affidabili ed esclusi**, quindi sulla scheda **Indirizzi IP esclusi**.

L'indirizzo IP verrà selezionato nell'elenco **Indirizzi IP esclusi**.

Gestione del registro eventi in ingresso

È possibile utilizzare la pagina **Eventi in ingresso** per gestire gli eventi del registro Eventi in ingresso generati quando il traffico Internet non richiesto viene bloccato da Personal Firewall.

Archiviazione del registro Eventi in ingresso

È possibile archiviare il registro degli eventi in ingresso corrente per salvare tutti gli eventi in ingresso registrati, incluse la data e le ore, gli IP di origine, i nomi di host, le porte e le informazioni sull'evento. Il registro degli eventi in ingresso va archiviato periodicamente per evitare che diventi troppo grande.

Per archiviare il registro Eventi in ingresso:

1. Fare clic con il pulsante destro del mouse sull'icona McAfee nella barra delle applicazioni di Windows, scegliere **Personal Firewall**, quindi selezionare **Eventi in ingresso**.
2. Nella pagina **Eventi in ingresso**, fare clic su **Archivio**.
3. Nella finestra di dialogo **Archivia registro**, fare clic su **Sì** per procedere con l'operazione.

4 Fare clic su **Salva** per salvare l'archivio nel percorso predefinito oppure scegliere un percorso in cui salvare l'archivio.

> **NOTA**
> Per impostazione predefinita, Personal Firewall archivia automaticamente il registro degli eventi in ingresso. Selezionare o deselezionare **Archivia automaticamente gli eventi registrati** nella pagina **Impostazioni registro eventi** per attivare o disattivare l'opzione.

Visualizzazione dei registri Eventi in ingresso archiviati

È possibile visualizzare i registri Eventi in ingresso archiviati in precedenza. L'archivio salvato include la data e le ore, gli IP di origine, i nomi host, le porte e le informazioni sugli eventi.

Per visualizzare il registro degli eventi in ingresso archiviato:

1 Fare clic con il pulsante destro del mouse sull'icona McAfee nella barra delle applicazioni di Windows, scegliere **Personal Firewall**, quindi selezionare **Eventi in ingresso**.

2 Nella pagina **Eventi in ingresso**, fare clic su **Visualizza archivi**.

3 Selezionare o cercare il nome file dell'archivio e fare clic su **Apri**.

Cancellazione del registro Eventi in ingresso

È possibile cancellare tutte le informazioni dal registro Eventi in ingresso.

> **ATTENZIONE**
> Una volta cancellato il registro Eventi in ingresso, non sarà possibile recuperarne il contenuto. Se si ritiene di averne bisogno in futuro, si consiglia di archiviare il Registro eventi anziché cancellarlo.

Per cancellare il registro Eventi in ingresso:

1 Fare clic con il pulsante destro del mouse sull'icona McAfee, scegliere **Personal Firewall**, quindi selezionare **Eventi in ingresso**.

2 Nella pagina **Eventi in ingresso**, fare clic su **Cancella registro**.

3 Fare clic su **Sì** nella finestra di dialogo per cancellare il registro.

Copia di un evento negli Appunti

È possibile copiare un evento negli Appunti per incollarlo in un file di testo utilizzando il Blocco note.

Per copiare gli eventi negli appunti:

1. Fare clic con il pulsante destro del mouse sull'icona McAfee, scegliere **Personal Firewall**, quindi selezionare **Eventi in ingresso**.
2. Fare clic con il pulsante destro del mouse sull'evento nel registro degli eventi in ingresso.
3. Fare clic su **Copia negli Appunti evento selezionato**.
4. Avviare Blocco note.
   - Digitare `notepad` nella riga di commando oppure fare clic su **Start**, scegliere **Programmi**, quindi **Accessori**. Selezionare **Blocco note**.
5. Scegliere **Incolla** dal menu **Modifica**. Il testo dell'evento verrà visualizzato nel Blocco note. Ripetere il passaggio fino a quando non saranno disponibili tutti gli eventi necessari.
6. Salvare il file del Blocco note in un percorso protetto.

Eliminazione dell'evento selezionato

È possibile eliminare eventi dal registro Eventi in ingresso.

Per eliminare eventi dal registro Eventi in ingresso:

1. Fare clic con il pulsante destro del mouse sull'icona McAfee nella barra delle applicazioni di Windows, scegliere **Personal Firewall**, quindi selezionare **Eventi in ingresso**.
2. Nella pagina **Eventi in ingresso**, fare clic sull'evento che si desidera eliminare.
3. Scegliere **Elimina evento selezionato** dal menu **Modifica**. L'evento viene eliminato dal registro eventi in ingresso.

Informazioni sugli avvisi

Si consiglia di acquisire familiarità con i tipi di avviso che verranno visualizzati durante l'utilizzo di Personal Firewall. Esaminare i seguenti tipi di avviso che possono essere visualizzati e le possibili risposte, in modo da poter reagire con sicurezza.

NOTA
I suggerimenti sugli avvisi aiutano a deciderne la gestione. Per visualizzare i suggerimenti sugli avvisi, fare clic sulla scheda **Opzioni**, sull'icona **Impostazioni avviso**, quindi selezionare **Usa suggerimenti intelligenti** (opzione predefinita) o **Visualizza solo suggerimenti intelligenti** dall'elenco **Suggerimenti intelligenti**.

Avvisi rossi

Gli avvisi rossi contengono informazioni importanti che richiedono l'attenzione immediata dell'utente:

- **Applicazione Internet bloccata**: questo avviso viene visualizzato se Personal Firewall blocca l'accesso a Internet di un'applicazione. Ad esempio, se viene visualizzato un avviso relativo a un programma cavallo di Troia, a tale programma viene automaticamente impedito l'accesso a Internet e all'utente viene consigliato di cercare i virus nel computer.
- **L'applicazione richiede l'accesso a Internet:** questo avviso viene visualizzato quando Personal Firewall rileva traffico Internet o di rete per le nuove applicazioni.
- **L'applicazione è stata modificata:** questo avviso viene visualizzato quando Personal Firewall rileva una modifica a un'applicazione a cui in precedenza era stato consentito l'accesso a Internet. Se l'applicazione non è stata aggiornata di recente, si consiglia di non concedere facilmente l'accesso a Internet all'applicazione modificata.

- **L'applicazione richiede l'Accesso server:** questo avviso viene visualizzato quando Personal Firewall rileva che un'applicazione a cui in precedenza era stato consentito l'accesso a Internet ha richiesto l'accesso a Internet come server.

  NOTA
  L'impostazione predefinita Aggiornamenti automatici di Windows XP SP2 scarica e installa gli aggiornamenti per il sistema operativo Windows e per gli altri programmi Microsoft eseguiti sul computer senza segnalarlo agli utenti. Quando un'applicazione viene modificata da uno degli aggiornamenti invisibili di Windows, gli avvisi di McAfee Personal Firewall vengono visualizzati al successivo avvio dell'applicazione Microsoft.

  IMPORTANTE
  È necessario consentire l'accesso alle applicazioni che richiedono l'accesso a Internet per scaricare gli ultimi aggiornamenti del prodotto online, quali i servizi di McAfee.

Avviso Applicazione Internet bloccata

Se viene visualizzato un avviso relativo a un programma cavallo di Troia (Figura 4-4), Personal Firewall impedisce automaticamente a tale programma l'accesso a Internet e all'utente viene consigliato di cercare i virus nel computer. Se non è installato McAfee VirusScan, è possibile avviare McAfee SecurityCenter.



Figura 4-4. Avviso Applicazione Internet bloccata

Visualizzare una breve descrizione dell'evento, quindi scegliere una delle seguenti opzioni:

- Fare clic su **Ulteriori informazioni** per ottenere informazioni dettagliate sull'evento consultando il registro Eventi in ingresso (per ulteriori informazioni vedere *Informazioni sulla pagina Eventi in ingresso* a pagina 98).
- Fare clic su **Avvia McAfee VirusScan** per cercare i virus nel computer.
- Fare clic su **Continuare l'operazione in corso** se non si desidera effettuare altre operazioni, oltre a quelle eseguite da Personal Firewall.
- Fare clic su **Consentire l'accesso in uscita** per consentire una connessione in uscita (protezione **Elevata**).

Avviso L'applicazione richiede l'accesso a Internet

Se si seleziona **Standard** o **Elevata** nelle opzioni **Impostazioni protezione**, viene visualizzato un avviso (Figura 4-5) quando vengono rilevate connessioni Internet o di rete per le applicazioni nuove o modificate.



Figura 4-5. Avviso L'applicazione richiede l'accesso a Internet

Se viene visualizzato un avviso in cui viene raccomandata attenzione nel consentire l'accesso dell'applicazione a Internet, è possibile fare clic su **Per ulteriori informazioni, fare clic qui** per ottenere ulteriori informazioni sull'applicazione. Questa opzione viene visualizzata nell'avviso solo se Personal Firewall è configurato per utilizzare i suggerimenti intelligenti.

McAfee potrebbe non riconoscere l'applicazione durante il tentativo di accesso a Internet (Figura 4-6).



Figura 4-6. Avviso Applicazione non riconosciuta

Pertanto, potrebbe non fornire indicazioni su come gestirla. È possibile segnalare l'applicazione a McAfee facendo clic su **Informa McAfee di questo programma**. Viene visualizzata una pagina Web in cui viene richiesto di inserire le informazioni relative all'applicazione. Inserire il maggior numero di informazioni disponibili.

Le informazioni inviate dagli utenti vengono utilizzate, in combinazione con altri strumenti di ricerca, dai nostri operatori HackerWatch per determinare se un'applicazione deve essere inserita nel nostro database di applicazioni note e, in tal caso, come deve essere gestita da Personal Firewall.

Visualizzare una breve descrizione dell'evento, quindi scegliere una delle seguenti opzioni:

- Fare clic su **Consentire l'accesso** per consentire all'applicazione di stabilire una connessione Internet in uscita e in ingresso.
- Fare clic su **Consenti accesso una volta sola** per concedere all'applicazione una connessione Internet temporanea. L'accesso è limitato all'intervallo che intercorre tra quando viene avviata l'applicazione e quando viene chiusa.
- Fare clic su **Bloccare tutti gli accessi** per impedire la connessione Internet.
- Fare clic su **Consentire l'accesso in uscita** per consentire una connessione in uscita (protezione **Elevata**).
- Fare clic su **Guida alla scelta** per visualizzare la Guida in linea sulle autorizzazioni di accesso delle applicazioni.

Avviso L'applicazione è stata modificata

Se è stata selezionata la protezione **Basata sull'affidabilità**, **Standard** o **Elevata** nelle opzioni **Impostazioni protezione**, viene visualizzato un avviso (Figura 4-7) quando Personal Firewall rileva una modifica in un'applicazione che in precedenza era stata autorizzata ad accedere a Internet. Se l'applicazione in questione non è stata aggiornata di recente, si consiglia di non concedere facilmente l'accesso a Internet all'applicazione modificata.



Figura 4-7. Avviso L'applicazione è stata modificata

Visualizzare una breve descrizione dell'evento, quindi scegliere una delle seguenti opzioni:

- Fare clic su **Consentire l'accesso** per consentire all'applicazione di stabilire una connessione Internet in uscita e in ingresso.
- Fare clic su **Consenti accesso una volta sola** per concedere all'applicazione una connessione Internet temporanea. L'accesso è limitato all'intervallo che intercorre tra quando viene avviata l'applicazione e quando viene chiusa.
- Fare clic su **Bloccare tutti gli accessi** per impedire la connessione Internet.
- Fare clic su **Consentire l'accesso in uscita** per consentire una connessione in uscita (protezione **Elevata**).
- Fare clic su **Guida alla scelta** per visualizzare la Guida in linea sulle autorizzazioni di accesso delle applicazioni.

Avviso L'applicazione richiede l'Accesso server

Se è stata selezionata la protezione **Elevata** nelle opzioni **Impostazioni protezione**, viene visualizzato un avviso (Figura 4-8) quando Personal Firewall rileva che un'applicazione, che in precedenza era stata autorizzata ad accedere a Internet, ha richiesto l'accesso a Internet come server.



Figura 4-8. Avviso L'applicazione richiede l'Accesso server

Ad esempio, un avviso viene visualizzato quando MSN Messenger richiede accesso al server per inviare un file durante una conversazione.

Visualizzare una breve descrizione dell'evento, quindi scegliere una delle seguenti opzioni:

- Fare clic su **Consenti accesso una volta sola** per consentire all'applicazione un accesso a Internet temporaneo. L'accesso è limitato all'intervallo che intercorre tra quando viene avviata l'applicazione e quando viene chiusa.
- Fare clic su **Consentire accesso server** per consentire all'applicazione di stabilire una connessione Internet in uscita e in ingresso.
- Fare clic su **Consentire solo accesso in uscita** per impedire le connessioni Internet in ingresso.
- Fare clic su **Bloccare tutti gli accessi** per impedire la connessione Internet.
- Fare clic su **Guida alla scelta** per visualizzare la Guida in linea sulle autorizzazioni di accesso delle applicazioni. Avvisi verdi

Avvisi verdi

Gli avvisi verdi indicano la presenza di eventi in Personal Firewall, come le applicazioni a cui è stato automaticamente concesso l'accesso a Internet.

Programma autorizzato all'accesso a Internet: questo avviso viene visualizzato quando l'accesso a Internet viene concesso automaticamente a tutte le applicazioni nuove e viene emessa una notifica (protezione **Basata sull'affidabilità**). Un esempio di applicazione modificata è un'applicazione con regole modificate per consentirne automaticamente l'accesso a Internet.

Avviso Applicazione autorizzata all'accesso a Internet

Se nelle opzioni **Impostazioni protezione** è stata selezionata la protezione **Basata sull'affidabilità**, Personal Firewall consente automaticamente l'accesso a Internet a tutte le applicazioni nuove, quindi informa l'utente con un avviso (Figura 4-9).



Figura 4-9. Programma autorizzato all'accesso a Internet

Visualizzare una breve descrizione dell'evento, quindi scegliere una delle seguenti opzioni:

- Fare clic su **Visualizzare registro applicazioni** per ottenere informazioni dettagliate sull'evento mediante il registro Eventi in ingresso applicazioni Internet (per ulteriori informazioni vedere *Informazioni sulla pagina Applicazioni Internet* a pagina 96).
- Per evitare la visualizzazione di questi tipi di avvisi, fare clic su **Disattivare tipo di avviso**.
- Fare clic su **Continuare l'operazione in corso** se non si desidera effettuare altre operazioni, oltre a quelle eseguite da Personal Firewall.
- Fare clic su **Bloccare tutti gli accessi** per impedire la connessione Internet.

Avviso L'applicazione è stata modificata

Se nelle opzioni **Impostazioni protezione** è stata selezionata la protezione **Basata sull'affidabilità**, Personal Firewall consente automaticamente l'accesso a Internet a tutte le applicazioni modificate. Visualizzare una breve descrizione dell'evento, quindi scegliere una delle seguenti opzioni:

- Fare clic su **Visualizzare registro applicazioni** per ottenere informazioni dettagliate sull'evento mediante il registro Eventi in ingresso applicazioni Internet (per ulteriori informazioni vedere *Informazioni sulla pagina Applicazioni Internet* a pagina 96).
- Per evitare la visualizzazione di questi tipi di avvisi, fare clic su **Disattivare tipo di avviso**.
- Fare clic su **Continuare l'operazione in corso** se non si desidera effettuare altre operazioni, oltre a quelle eseguite da Personal Firewall.
- Fare clic su **Bloccare tutti gli accessi** per impedire la connessione Internet.

Avvisi blu

Gli avvisi blu contengono informazioni, ma non richiedono una reazione da parte dell'utente.

- **Tentativo di connessione bloccato:** questo avviso viene visualizzato quando il traffico Internet o di rete indesiderato viene bloccato da Personal Firewall (Protezione basata su affidabilità, standard o elevata).

Avviso Tentativo di connessione bloccato

Se è stata seleziona la protezione **Basata sull'affidabilità**, **Standard** o **Elevata**, viene visualizzato un avviso (Figura 4-10) in caso di blocco del traffico Internet o di rete indesiderato.



Figura 4-10. Avviso Tentativo di connessione bloccato

Visualizzare una breve descrizione dell'evento, quindi scegliere una delle seguenti opzioni:

- Fare clic su **Visualizzare registro eventi** per ottenere informazioni dettagliate sull'evento mediante il registro Eventi in ingresso di Personal Firewall (per ulteriori informazioni vedere *Informazioni sulla pagina Eventi in ingresso* a pagina 98).
- Fare clic su **Rintracciare questo indirizzo** per creare una traccia visuale degli indirizzi IP relativi all'evento.
- Fare clic su **Escludere questo indirizzo** per bloccare l'accesso al computer di questo indirizzo. L'indirizzo verrà aggiunto all'elenco **Indirizzi IP esclusi**.
- Fare clic su **Accettare come affidabile** per consentire l'accesso di questo indirizzo IP al computer.
- Fare clic su **Continuare l'operazione in corso** se non si desidera effettuare altre operazioni, oltre a quelle eseguite da Personal Firewall.

Indice

O

P

Q

R

S